ESET MAIL SECURITY

FOR MICROSOFT EXCHANGE SERVER

Installation Manual and User Guide

Microsoft® Windows® Server 2000 / 2003 / 2008 / 2008 R2 / 2012

Click here to download the most recent version of this document

ESET **MAIL SECURITY**

Copyright ©2013 by ESET, spol. s r.o.
ESET Mail Security was developed by ESET, spol. s r.o.

For more information visit www.eset.com.
All rights reserved. No part of this documentation may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning, or otherwise without permission in writing from the author.
ESET, spol. s r.o. reserves the right to change any of the described application software without prior notice.

Customer Care: www.eset.com/support

REV. 11/7/2013

Contents

1. Introduction....5

1.1 What's new in version 4.5 ?....5
1.2 System requirements....5
1.3 Methods used....6
1.3.1 Mailbox scanning via VSAPI....6
1.3.2 Message filtering on the SMTP server level....6
1.4 Types of protection....6
1.4.1 Antivirus protection....6
1.4.2 Antispam protection....6
1.4.3 Application of user-defined rules....7
1.5 User interface....7

2. Installation....8

2.1 Typical Installation....8
2.2 Custom Installation....9
2.3 Terminal Server....11
2.4 Upgrading to a newer version....11
2.5 Exchange Server Roles - Edge vs Hub....12
2.6 Exchange Server 2013 Roles....13
2.7 Installation in a clustered environment....13
2.8 License....15
2.9 Post-Installation Configuration....17

3. ESET Mail Security - Microsoft Exchange Server protection....19

3.1 General settings....19
3.1.1 Microsoft Exchange Server....19
3.1.1.1 VSAPI (Virus-Scanning Application Programming Interface)....19
3.1.1.2 Transport Agent....19
3.1.2 Rules....20
3.1.2.1 Adding new rules....21
3.1.2.2 Actions taken when applying rules....22
3.1.3 Log files....23
3.1.4 Message quarantine....24
3.1.4.1 Adding a new quarantine rule....25
3.1.5 Performance....25
3.2 Antivirus and antispyware settings....26
3.2.1 Microsoft Exchange Server....26
3.2.1.1 Virus-Scanning Application Programming Interface (VSAPI)....27
3.2.1.1.1 Microsoft Exchange Server 5.5 (VSAPI 1.0)....27
3.2.1.1.1.1 Actions....27
3.2.1.1.1.2 Performance....27
3.2.1.1.2 Microsoft Exchange Server 2000 (VSAPI 2.0)....27
3.2.1.1.2.1 Actions....28
3.2.1.1.2.2 Performance....28
3.2.1.1.3 Microsoft Exchange Server 2003 (VSAPI 2.5)....29
3.2.1.1.3.1 Actions....29
3.2.1.1.3.2 Performance....30
3.2.1.1.4 Microsoft Exchange Server 2007/2010 (VSAPI 2.6)..30
3.2.1.1.4.1 Actions....31
3.2.1.1.4.2 Performance....31
3.2.1.1.5 Transport Agent....32
3.2.2 Actions....33
3.2.3 Alerts and notifications....33
3.2.4 Automatic exclusions....34
3.3 Antispam protection....35
3.3.1 Microsoft Exchange Server....36
3.3.1.1 Transport Agent....36
3.3.1.2 POP3 Connector and antispam....37
3.3.2 Antispam engine....38
3.3.2.1 Antispam engine parameter setup....38
3.3.2.1.1 Analysis....38
3.3.2.1.1.1 Samples....39
3.3.2.1.1.2 SpamCompiler....39
3.3.2.1.1.1 List of cache memory files....39
3.3.2.1.2 Training....39
3.3.2.1.3 Rules....40
3.3.2.1.3.1 Rule weight....40
3.3.2.1.3.1 Add rule weight....41
3.3.2.1.3.2 List of downloaded rule files....41
3.3.2.1.3.3 Category weight....41
3.3.2.1.3.1 Add category weight....41
3.3.2.1.3.4 Custom rules list....41
3.3.2.1.4 Filtering....41
3.3.2.1.4.1 Allowed senders....42
3.3.2.1.4.2 Blocked senders....42
3.3.2.1.4.3 Allowed IP addresses....42
3.3.2.1.4.4 Ignored IP addresses....42
3.3.2.1.4.5 Blocked IP addresses....42
3.3.2.1.4.6 Allowed domains....42
3.3.2.1.4.7 Ignored domains....43
3.3.2.1.4.8 Blocked domains....43
3.3.2.1.4.9 Spoofed senders....43
3.3.2.1.5 Verification....43
3.3.2.1.5.1 RBL (Realtime Blackhole List)....43
3.3.2.1.5.1 List of RBL servers....43
3.3.2.1.5.2 LBL (Last Blackhole List)....44
3.3.2.1.5.1 List of LBL servers....44
3.3.2.1.5.2 List of skipped IP addresses....44
3.3.2.1.5.3 DNSBL (DNS Block List)....44
3.3.2.1.5.1 List of DNSBL servers....44
3.3.2.1.6 DNS....44
3.3.2.1.7 Score....45
3.3.2.1.8 Spambait....45
3.3.2.1.8.1 Spambait addresses....45
3.3.2.1.8.2 Addresses regarded as nonexistent....45
3.3.2.1.9 Communication....45
3.3.2.1.10 Performance....46
3.3.2.1.11 Regional settings....46
3.3.2.1.11.1 List of home languages....46
3.3.2.1.11.2 List of home countries....48
3.3.2.1.11.3 List of blocked countries....52
3.3.2.1.11.4 List of blocked charsets....52
3.3.2.1.12 Log files....52
3.3.2.1.13 Statistics....52
3.3.2.1.14 Options....52
3.3.3 Alerts and notifications....53
3.4 FAQ....53

4. ESET Mail Security - Server protection...56

4.1 Antivirus and antispyware protection....56
4.1.1 Real-time file system protection....56
4.1.1.1 Control setup....56
4.1.1.1.1 Media to scan....57
4.1.1.1.2 Scan on (Event-triggered scanning)....57
4.1.1.1.3 Advanced scan options....57
4.1.1.2 Cleaning levels....57
4.1.1.3 When to modify real-time protection configuration....58
4.1.1.4 Checking real-time protection....58
4.1.1.5 What to do if real-time protection does not work....58
4.1.2 Email client protection....59
4.1.2.1 POP3 checking....59
4.1.2.1.1 Compatibility....60
4.1.2.2 Integration with email clients....61
4.1.2.2.1 Appending tag messages to email body....62
4.1.2.3 Removing infiltrations....62
4.1.3 Web access protection....63
4.1.3.1 HTTP, HTTPs....63
4.1.3.1.1 Address management....64
4.1.3.1.2 Active mode....65

4.1.4 On-demand computer scan....66
4.1.4.1 Type of scan....67
4.1.4.1.1 Smart scan....67
4.1.4.1.2 Custom scan....67
4.1.4.2 Scan targets....68
4.1.4.3 Scan profiles....68
4.1.4.4 Command Line....69
4.1.5 Performance....71
4.1.6 Protocol filtering....71
4.1.6.1 SSL....71
4.1.6.1.1 Trusted certificates....72
4.1.6.1.2 Excluded certificates....72
4.1.7 ThreatSense engine parameters setup....72
4.1.7.1 Objects setup....73
4.1.7.2 Options....73
4.1.7.3 Cleaning....74
4.1.7.4 Extensions....75
4.1.7.5 Limits....76
4.1.7.6 Other....76
4.1.8 An infiltration is detected....77
4.2 Updating the program....78
4.2.1 Update setup....79
4.2.1.1 Update profiles....80
4.2.1.2 Advanced update setup....80
4.2.1.2.1 Update mode....81
4.2.1.2.2 Proxy server....82
4.2.1.2.3 Connecting to the LAN....84
4.2.1.2.4 Creating update copies - Mirror....85
4.2.1.2.4.1 Updating from the Mirror....86
4.2.1.2.4.2 Troubleshooting Mirror update problems....87
4.2.2 How to create update tasks....87
4.3 Scheduler....88
4.3.1 Purpose of scheduling tasks....88
4.3.2 Creating new tasks....89
4.4 Quarantine....90
4.4.1 Quarantining files....90
4.4.2 Restoring from Quarantine....90
4.4.3 Submitting file from Quarantine....91
4.5 Log files....92
4.5.1 Log filtering....96
4.5.2 Find in log....97
4.5.3 Log maintenance....98
4.6 ESET SysInspector....99
4.6.1 Introduction to ESET SysInspector....99
4.6.1.1 Starting ESET SysInspector....99
4.6.2 User Interface and application usage....100
4.6.2.1 Program Controls....100
4.6.2.2 Navigating in ESET SysInspector....101
4.6.2.2.1 Keyboard shortcuts....102
4.6.2.3 Compare....104
4.6.3 Command line parameters....105
4.6.4 Service Script....105
4.6.4.1 Generating Service script....105
4.6.4.2 Structure of the Service script....106
4.6.4.3 Executing Service scripts....108
4.6.5 FAQ....108
4.6.6 ESET SysInspector as part of ESET Mail Security....109
4.7 ESET SysRescue....110
4.7.1 Minimum requirements....110
4.7.2 How to create rescue CD....110
4.7.3 Target selection....111
4.7.4 Settings....111
4.7.4.1 Folders....111
4.7.4.2 ESET Antivirus....111
4.7.4.3 Advanced settings....112
4.7.4.4 Internet protocol....112
4.7.4.5 Bootable USB device....112
4.7.4.6 Burn....112
4.7.5 Working with ESET SysRescue....113
4.7.5.1 Using ESET SysRescue....113
4.8 User interface options....113
4.8.1 Alerts and notifications....115
4.8.2 Disable GUI on Terminal Server....116
4.9 eShell....116
4.9.1 Usage....117
4.9.2 Commands....120
4.10 Import and export settings....122
4.11 ThreatSense.Net....122
4.11.1 Suspicious files....124
4.11.2 Statistics....125
4.11.3 Submission....126
4.12 Remote administration....127
4.13 Licenses....128
5. Glossary....129
5.1 Types of infiltration....129
5.1.1 Viruses....129
5.1.2 Worms....129
5.1.3 Trojan horses....129
5.1.4 Rootkits....130
5.1.5 Adware....130
5.1.6 Spyware....130
5.1.7 Potentially unsafe applications....131
5.1.8 Potentially unwanted applications....131
5.2 Email....131
5.2.1 Advertisements....132
5.2.2 Hoaxes....132
5.2.3 Phishing....132
5.2.4 Recognizing spam scams....132
5.2.4.1 Rules....133
5.2.4.2 Bayesian filter....133
5.2.4.3 Whitelist....133
5.2.4.4 Blacklist....133
5.2.4.5 Server-side control....134

1. Introduction

ESET Mail Security 4 for Microsoft Exchange Server is an integrated solution that protects mailboxes from various types of malware content including email attachments infected by worms or trojans, documents containing harmful scripts, phishing and spam. ESET Mail Security provides three types of protection: Antivirus, Antispam and the application of user-defined rules. ESET Mail Security filters the malicious content at the mail server level, before it arrives in the recipient's email client inbox.

ESET Mail Security supports Microsoft Exchange Server versions 2000 and later, as well as Microsoft Exchange Server in a cluster environment. In newer versions (Microsoft Exchange Server 2007 and later), specific roles (mailbox, hub, edge) are also supported. You can remotely manage ESET Mail Security in larger networks with the help of ESET Remote Administrator.

While providing Microsoft Exchange Server protection, ESET Mail Security also has tools to ensure protection of the server itself (resident protection, web-access protection, email client protection and antispam).

1.1 What's new in version 4.5 ?

Compared with ESET Mail Security version 4.3 the following novelties and improvements have been introduced in the version 4.5:

- Antispam settings - easily accessible from the GUI to make changes much more convenient for administrators
- Support for Microsoft Exchange Server 2013
- Support for Microsoft Windows Server 2012

1.2 System requirements

Supported Operating Systems:

- Microsoft Windows 2000 Server
- Microsoft Windows Server 2003 (x86 and x64)
- Microsoft Windows Server 2008 (x86 and x64)
- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2012
- Microsoft Windows Small Business Server 2003 (x86)
- Microsoft Windows Small Business Server 2003 R2 (x86)
- Microsoft Windows Small Business Server 2008 (x64)
- Microsoft Windows Small Business Server 2011 (x64)

Supported Microsoft Exchange Server versions:

- Microsoft Exchange Server 2000 SP1, SP2, SP3
- Microsoft Exchange Server 2003 SP1, SP2
- Microsoft Exchange Server 2007 SP1, SP2, SP3
- Microsoft Exchange Server 2010 SP1, SP2, SP3
- Microsoft Exchange Server 2013

Hardware requirements depend on the operating system version and the version of Microsoft Exchange Server in use. We recommend reading the Microsoft Exchange Server product documentation for more detailed information on hardware requirements.

1.3 Methods used

Two independent methods are used to scan email messages:

Mailbox scanning via VSAPI 6
Message filtering on the SMTP server level 6

1.3.1 Mailbox scanning via VSAPI

The mailbox scanning process is triggered and controlled by the Microsoft Exchange Server. Emails in the Microsoft Exchange Server store database are scanned continuously. Depending on the version of Microsoft Exchange Server, the VSAPI interface version and the user-defined settings, the scanning process can be triggered in any of the following situations:

- When the user accesses email, e.g. in an email client (email is always scanned with the latest virus signature database)
- In the background, when use of the Microsoft Exchange Server is low
- Proactively (based on the Microsoft Exchange Server's inner algorithm)

The VSAPI interface is currently used for antivirus scan and rule-based protection.

1.3.2 Message filtering on the SMTP server level

SMTP server-level filtering is secured by a specialized plugin. In Microsoft Exchange Server 2000 and 2003, the plugin in question (*Event Sink*) is registered on the SMTP server as a part of Internet Information Services (IIS). In Microsoft Exchange Server 2007/2010, the plugin is registered as a transport agent on the *Edge* or the *Hub* roles of the Microsoft Exchange Server.

SMTP server-level filtering by a transport agent provides protection in the form of antivirus, antispam and user-defined rules. As opposed to VSAPI filtering, the SMTP server-level filtering is performed before the scanned email arrives in the Microsoft Exchange Server mailbox.

1.4 Types of protection

There are three types of protection:

1.4.1 Antivirus protection

Antivirus protection is one of the basic functions of the ESET Mail Security product. Antivirus protection guards against malicious system attacks by controlling file, email and Internet communication. If a threat with malicious code is detected, the Antivirus module can eliminate it by blocking it and then cleaning, deleting or moving it to quarantine 90.

1.4.2 Antispam protection

Antispam protection integrates several technologies (RBL, DNSBL, Fingerprinting, Reputation checking, Content analysis, Bayesian filtering, Rules, Manual whitelisting/blacklisting, etc.) to achieve maximum detection of email threats. The antispam scanning engine's output is the spam probability value of the given email message expressed as a percentage (0 to 100).

Another component of the antispam protection module is the Greylisting technique (disabled by default). The technique relies on the RFC 821 specification, which states that since SMTP is considered an unreliable transport, every message transfer agent (MTA) should repeatedly attempt to deliver an email after encountering a temporary delivery failure. A substantial part of spam consists of one-time deliveries (using specialized tools) to a bulk list of email addresses generated automatically. A server employing Greylisting calculates a control value (hash) for the envelope sender address, the envelope recipient address and the IP address of the sending MTA. If the server cannot find the control value for the triplet within its own database, it refuses to accept the message, returning a temporary failure code (temporary failure, for example, 451). A legitimate server will attempt a redelivery of the message after a variable time period. The triplet's control value will be stored in the database of verified connections on the second attempt, allowing any email with relevant characteristics to be delivered from then on.

1.4.3 Application of user-defined rules

Protection based on user-defined rules is available for scanning with both the VSAPI and the transport agent. You can use the ESET Mail Security user interface to create individual rules that may also be combined. If one rule uses multiple conditions, the conditions will be linked using the logical operator AND. Consequently, the rule will be executed only if all its conditions are fullfilled. If multiple rules are created, the logical operator OR will be applied, meaning the program will run the first rule for which the conditions are met.

In the scanning sequence, the first technique used is greylisting - if it is enabled. Consequent procedures will always execute the following techniques: protection based on user-defined rules, followed by an antivirus scan and, lastly, an antispam scan.

1.5 User interface

ESET Mail Security has graphical user interface (GUI) designed to be as intuitive as possible. The GUI gives users quick and easy access to the main functions of the program.

In addition the main GUI, there is an **advanced setup tree** which is accessible from anywhere in the program by pressing the F5 key.

Once you press F5, the advanced setup tree window opens and displays a list of configurable program features. From this window, you can configure the settings and options based on your needs. The tree structure is split into two main sections: **Server protection** and **Computer protection**. Apart from that, there are several other sections such as Update, Tools, User interface and Miscellaneous. The **Server protection** section contains items concerning ESET Mail Security settings, specific for Microsoft Exchange server protection. The **Computer protection** section contains the configurable items for the protection of the server itself.

2. Installation

After purchasing ESET Mail Security, the installer can be downloaded from ESET's website (www.eset.com) as an .msi package.

Please note that you need to execute the installer under **Built-in Administrator** account. Any other user, despite being a member of Administrators group, will not have sufficient access rights. Therefore you need to use Built-in Administrator account, as you will not be able to successfully complete the installation under any other user account than **Administrator**.

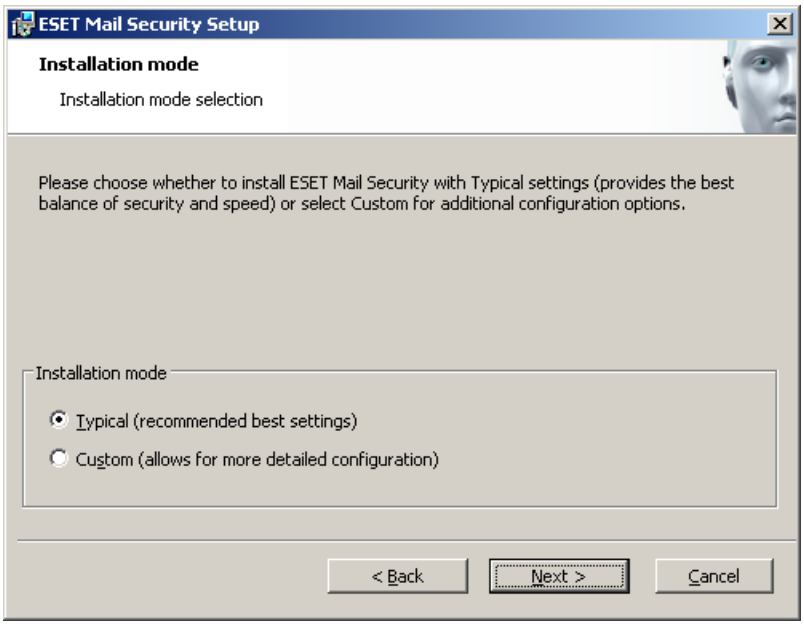
There are two ways to execute the installer:

- You can login locally using Administrator account credentials and simply run the installer
- You can be logged in as other user, but need to open command prompt with **Run as...** and type in Administrator account credentials to have the cmd running as Administrator, then type in the command to execute the installer (e.g. `msiexec /i emsx_nt64_ENU.msi` but you need to replace `emsx_nt64_ENU.msi` with the exact file name of the msi installer you have downloaded)

Once you launch the installer, the installation wizard will guide you through the basic setup. There are two types of installation available with different levels of setup details:

1. **Typical Installation**

2. **Custom Installation**


ESET Mail Security Setup
Installation mode
Installation mode selection
Please choose whether to install ESET Mail Security with Typical settings (provides the best balance of security and speed) or select Custom for additional configuration options.
Installation mode
Typical (recommended best settings)
Custom (allows for more detailed configuration)
< Back
Next >
Cancel

NOTE: We highly recommend installing ESET Mail Security on a freshly installed and configured OS, if possible. However, if you do need to install it on an existing system, the best to do is to uninstall previous version of ESET Mail Security, restart the server and install the new ESET Mail Security afterwards.

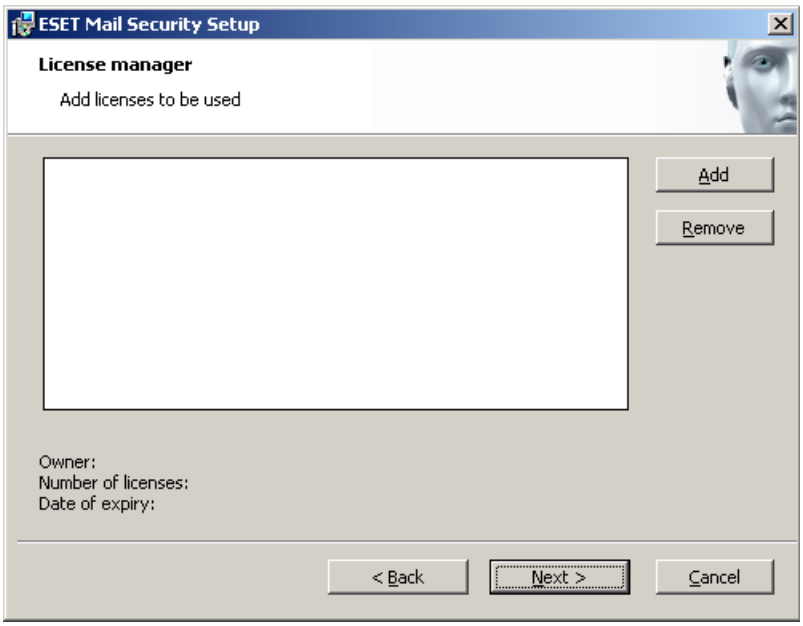
2.1 Typical Installation

Typical installation mode quickly installs ESET Mail Security with minimal configuration during the installation process. Typical installation is the default installation mode and is recommended if you do not have particular requirements for specific settings yet. After ESET Mail Security has been installed on your system, you can modify the options and configuration settings at any time. This user guide describes these settings and functionality in detail. The Typical installation mode settings provide excellent security coupled with ease of use and high system performance.

After selecting the installation mode and clicking Next, you will be prompted to enter your Username and Password. This plays a significant role in providing constant protection to your system, as your Username and Password allows automatic virus signature database Updates 78.

Enter the Username and Password, which you received after the purchase or registration of the product, into the corresponding fields. If you do not currently have your Username and Password available, it can be entered directly from the program at a later time.

In the next step - **License Manager** - Add the license file that was delivered via email after you purchased your product.



The next step is to configure the ThreatSense.Net Early Warning System. The ThreatSense.Net Early Warning System helps ensure that ESET is immediately and continuously informed about new infiltrations in order to quickly protect its customers. This system allows new threats to be submitted to ESET's Threat Lab, where they are analyzed, processed and added to the virus signature database. By default, the **Enable ThreatSense.Net Early Warning System** option is selected. Click **Advanced setup...** to modify detailed settings about the submission of suspicious files.

The next step in the installation process is to configure **Detection of potentially unwanted applications**. Potentially unwanted applications are not necessarily malicious, but can often negatively affect the behavior of your operating system. See the Potentially unwanted applications 131 chapter for more details.

These applications are often bundled with other programs and may be difficult to notice during the installation process. Although these applications usually display a notification during installation, they can easily be installed without your consent.

Select the **Enable detection of potentially unwanted applications** option to allow ESET Mail Security to detect this type of applications. If you do not whish to use this functionality, select **Disable detection of potentially unwanted applications.**

The final step in Typical installation mode is to confirm the installation by clicking the **Install** button.

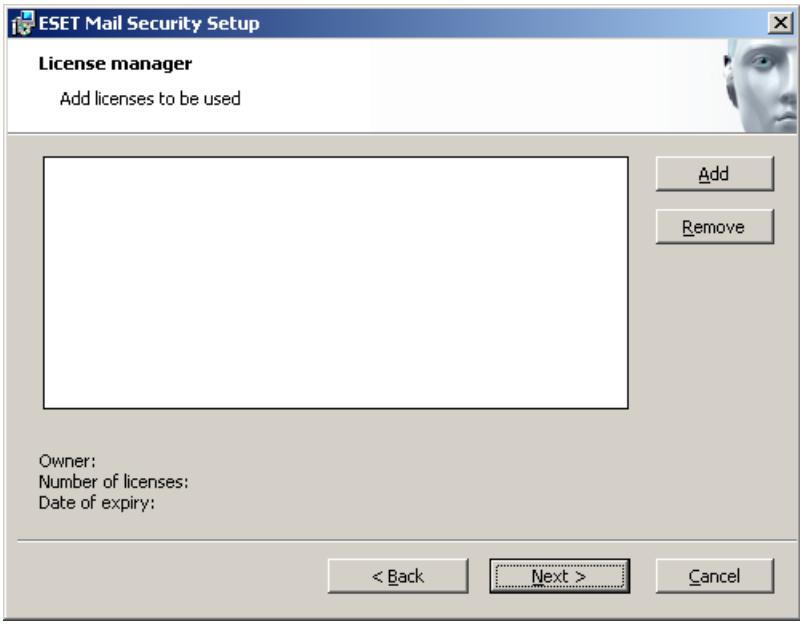
2.2 Custom Installation

Custom installation is designed for those who would like to configure ESET Mail Security during the installation process.

After selecting the installation mode and clicking **Next**, you will be prompted to select a destination location for the installation. By default, the program installs in *C:\Program Files\ESET\ESET Mail Security*. Click **Browse...** to change this location (not recommended).

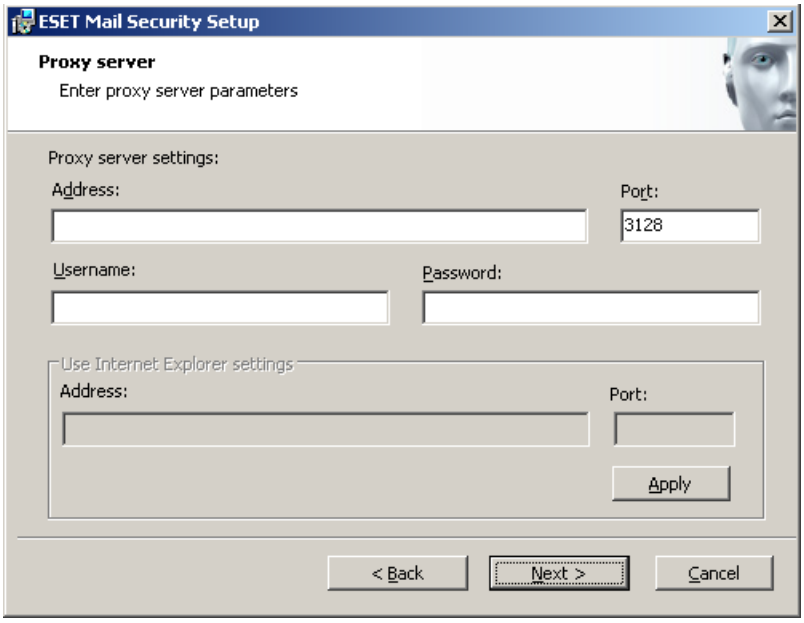
Next, enter your **Username** and **Password**. This step is the same as the Typical installation mode step (see "Typical installation" 8).

In the next step - **License Manager** - Add the license file that was delivered via email after you purchased your product.



After entering your Username and Password, click **Next** to proceed to **Configure your Internet connection**.

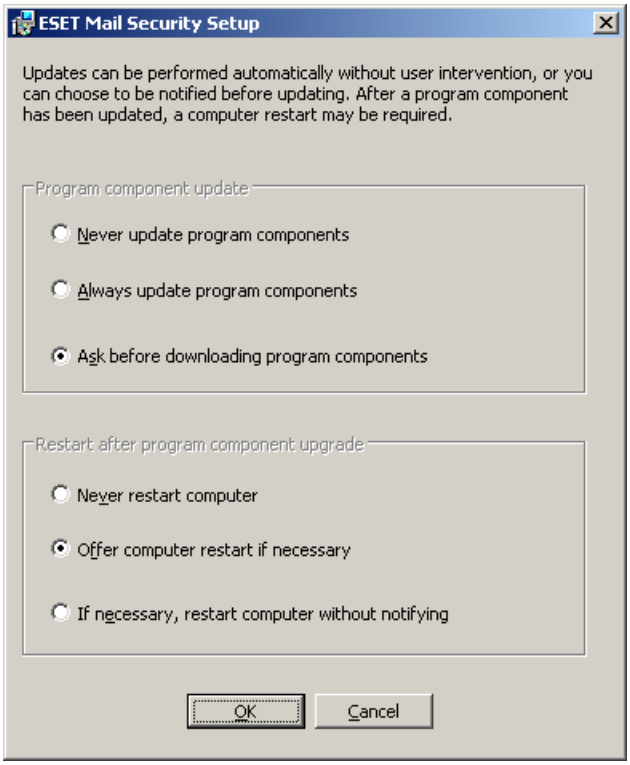
If you use a proxy server, it must be correctly configured for virus signature updates to work correctly. If you would like to have the proxy server configured automatically, select the default setting **I am unsure if my Internet connection uses a proxy server. Use the same settings as Internet Explorer (Recommended)** and click **Next**. If you do not use a proxy server, select the **I do not use a proxy server** option.



If you prefer to enter the proxy server details yourself, you can configure the proxy server settings manually. To configure your proxy server settings, select **I use a proxy server** and click **Next**. Enter the IP address or URL of your proxy server in the **Address** field. In the **Port** field, specify the port where the proxy server accepts connections (3128 by default). If your proxy server requires authentication, enter a valid **Username** and **Password** to grant access to the proxy server. Proxy server settings can also be copied from Internet Explorer if desired. Once the proxy server details are entered, click **Apply** and confirm the selection.

Click **Next** to proceed to **Configure automatic update** settings. This step allows you to designate how automatic program component updates will be handled on your system. Click **Change...** to access the advanced settings.

If you do not want program components to be updated, select the **Never update program components** option. Select the **Ask before downloading program components** option to display a confirmation window before downloading program components. To download program component upgrades automatically, select the **Always update program components** option.


ESET Mail Security Setup
Updates can be performed automatically without user intervention, or you can choose to be notified before updating. After a program component has been updated, a computer restart may be required.
Program component update
Never update program components
Always update program components
Ask before downloading program components
Restart after program component upgrade
Never restart computer
Offer computer restart if necessary
If necessary, restart computer without notifying
OK
Cancel

NOTE: After a program component update, a restart is usually required. We recommend selecting the **Never restart computer** option. The latest component updates will come into effect after the next server restart (whether it is scheduled 88, manual or otherwise). You can choose **Offer computer restart if necessary** if you would like to be reminded to restart the server after the components were updated. With this setting, you can restart the server right away or postpone the restart and perform it at a later time.

The next installation window offers the option to set a password to protect your program settings. Select the **Protect configuration settings with a password** option and choose a password to enter in the **New password** and **Confirm new password** fields.

The next three installation steps, **ThreatSense.Net Early Warning System**, **Detection of potentially unwanted applications** are the same as the Typical installation mode steps (see "Typical installation" 8).

Click **Install** in the **Ready to install** window to complete installation.

2.3 Terminal Server

If you are installing ESET Mail Security on Windows Server that acts as a Terminal Server, you might want to disable the ESET Mail Security GUI to prevent it from starting up every time a user logs in. See Disable GUI on Terminal Server 116 for specific steps to disable the GUI.

2.4 Upgrading to a newer version

Newer versions of ESET Mail Security are issued to provide improvements or fix issues that cannot be resolved through automatic program module updates. You can upgrade to the latest version of ESET Mail Security using the following methods:

1. Automatically upgrade by means of a program component update (PCU)
   Since program component updates are distributed to all users and may have an impact on certain system configurations, they are issued after a long period of testing to ensure a smooth upgrade process on all possible system configurations.
2. Manually, for example in the case that you need to upgrade to a newer version immediately after it has been released, or if you want to upgrade to the next generation of ESET Mail Security (e.g. from version 4.2 or 4.3 to version 4.5).

You can perform a manual upgrade to a newer version in two ways, in-place (the latest version is installed over your existing version) or using a clean installation (the previous version is uninstalled first and then the latest version is

installed).

To perform a manual upgrade:

1. In-place upgrade: Install the latest version over your existing version of ESET Mail Security by following the steps in the Installation 8 chapter. All existing settings (including antispam settings) will automatically be imported into the newer version during installation.

2. Clean installation:

a) Export your configuration/settings to an xml file using the Import and export settings 122 feature.

b) Open this xml file in a dedicated xml editor or a text editor that support xml (e.g. WordPad, Nodepad++, etc.), then change the third line SECTION ID number to "1000404" so that it looks like this:

```
<SECTION ID="1000404">
```

c) Download the EMSX AntispamSettingsExport tool from this Knowledgebase article. Save `EMSX_AntispamSettingsExport.exe` to the Exchange Server you are upgrading to the latest version of ESET Mail Security.

d) Run the `EMSX_AntispamSettingsExport.exe` tool. The tool will create a `cfg.xml` file containing the antispam settings from your existing installation of ESET Mail Security.

e) Download the msi installer file for the latest version of ESET Mail Security.

f) Copy the `cfg.xml` file created by the EMSX AntispamSettingsExport tool to the same location where you saved the ESET Mail Security msi installer file (e.g. `emsx_nt64_ENU.msi`).

g) Uninstall your existing version of ESET Mail Security.

h) Run the msi installer for ESET Mail Security 4.5. Antispam settings exported to `cfg.xml` will automatically be imported to the new version.

i) Once the installation is complete, import the configuration/settings from the xml file that you saved and modified in steps a) and b) using the Import and export settings 122 feature and an xml editor so that you can use your previous configuration settings in the new version of ESET Mail Security.

After performing the steps above, you will have the new version of ESET Mail Security installed on your system with your previous custom configuration.

For more details regarding upgrade process see this Knowledgebase article.

NOTE: Both manual upgrade processes (in-place and clean installation) apply to the upgrade from ESET Mail Security version 4.2 or 4.3 to ESET Mail Security version 4.5 only.

2.5 Exchange Server Roles - Edge vs Hub

By default, an Edge Transport server has its antispam features enabled and a Hub Transport server has its antispam features disabled. In an Exchange organization with Edge Transport server, this is the desired configuration. We recommend that you have the Edge Transport server running ESET Mail Security antispam configured to filter messages before they are routed into the Exchange organization.

The Edge role is the preferred location for antispam scanning because it allows ESET Mail Security to reject spam early in the process without putting an unnecessary load on network layers. Using this configuration, incoming messages are filtered by ESET Mail Security on the Edge Transport server, so they can safely be moved to the Hub Transport server without the need for further filtering.

If your organization does not use an Edge Transport server and has only a Hub Transport server, we recommend that you enable antispam features on the Hub Transport server that receives inbound messages from the Internet via SMTP.

2.6 Exchange Server 2013 Roles

The architecture of Exchange Server 2013 is different from previous versions of Microsoft Exchange. In Exchange 2013 there are only two server roles, Client Access server and Mailbox server. If you are planning to protect Microsoft Exchange 2013 with ESET Mail Security, make sure to install ESET Mail Security on a system running Microsoft Exchange 2013 with the Mailbox server role. The Client Access server role is not supported by ESET Mail Security. If you install ESET Mail Security on a system running with Client Access server role, there is a possibility that some features will not work, or will function incorrectly.

NOTE: Due to certain technical restrictions of Microsoft Exchange 2013, ESET Mail Security does not support the Client Access server (CAS) role.

2.7 Installation in a clustered environment

A cluster is a group of servers (a server connected to a cluster is called a "node") that work together as a single server. This type of environment provides high accessibility and reliability of available services. If one of the nodes in the cluster fails or becomes inaccessible, its functioning is automatically covered by another node in the cluster. ESET Mail Security fully supports Microsoft Exchange Servers connected in a cluster. In order for ESET Mail Security to function properly, it is important that each node in a cluster contains the same configuration. This can be achieved by applying a policy using ESET Remote Administrator (ERA). In the following chapters we will describe how to install and configure ESET Mail Security on servers in a clustered environment using ERA.

Installation

This chapter explains the push installation method; however this is not the only way to install a product on the target computer. For information on additional installation methods, refer to the ESET Remote Administrator User Guide.

1) Download the ESET Mail Security *msi* installation package from the ESET website to the computer where ERA is installed. In ERA > **Remote Install** tab > **Computers**, right-click on any computer from the list and choose **Manage Packages** from the context menu. In the **Type** drop-down menu, select **ESET Security Products package** and click **Add...** In the **Source**, locate the downloaded ESET Mail Security installation package and click **Create**.

2) In **Edit/Select configuration associated with this package**, click **Edit** and configure the settings of **ESET Mail Security** according to your needs. ESET Mail Security settings are in the following branches: **ESET Smart Security, ESET NOD32 Antivirus > Mail server protection** and **Mail server protection for Microsoft Exchange Server**. You may also set the parameters of other modules included in ESET Mail Security (e.g., Update module, Computer scan, etc.). We recommend exporting configured settings into an xml file which you can later use, e.g. when creating installation package, applying Configuration Task or a Policy.

3) Click **Close**. In the next dialog window (**Do you want to save the package into server?**) select **Yes** and type the name of the installation package. The finished installation package (including name and configuration) will be saved on the server. Most frequently, this package is used for a Push Installation, but it is also possible to save it as a standard *msi* installation package and use it for a direct installation on the server (in the **Installation Packages Editor** > **Save As...**).

4) Now that the installation package is ready, you can initiate the remote installation on the nodes within a cluster. In the ERA > **Remote Install** tab > **Computers**, select the nodes on which you want to install ESET Mail Security (Ctrl + Left-click or Shift + Left-click). Right-click on any of selected computers and select **Push Installation** from the context menu. Using the **Set** / **Set All** buttons, set the **Username** and **Password** of a user on the target computer (this must be a user with administrator rights). Click **Next** to choose the installation package and initiate the remote installation process by clicking **Finish**. The installation package containing ESET Mail Security and custom configuration settings will be installed on selected target computers/nodes. After a short time, clients with ESET Mail Security will appear in the ERA > **Clients** tab. You may now manage the clients remotely.

NOTE: For a seamless remote installation process, it is necessary to fulfill certain conditions on the target computers as well as on the ERA Server. For further details, refer to the ESET Remote Administrator User Guide.

Configuration

For ESET Mail Security to function correctly on the nodes within a cluster, the nodes must have the same configuration at all times. This condition is met if you followed the push installation method above. However, there is a chance that the configuration will be changed by mistake, causing inconsistencies between ESET Mail Security

products within a cluster. You can avoid this by using a policy in ERA. A policy is very similar to a standard Configuration Task – it sends the configuration defined in the Configuration Editor to the client(s). A policy is different from a Configuration Task because it is continuously applied to the client(s). So the Policy can be defined as a configuration that is regularly forced to a client / group of clients.

In ERA > **Tools** > **Policy Manager...** there is a number of options on how to use a policy. The easiest option is to use **Default Parent Policy** which also generally serves as **Default policy for primary clients**. This kind of policy is automatically applied to all currently connected clients (in this case, to all ESET Mail Security products within a cluster). You can configure the Policy by clicking **Edit...**, or use existing configuration saved in the *xml* file, if you have already created one.

The second option is to create a new policy (**Add New Child Policy**) and use the **Add Clients...** option to assign all ESET Mail Security products to this policy.

This configuration ensures a single policy with the same settings will be applied to all clients. If you wish to modify existing settings of an ESET Mail Security server within a cluster, it is sufficient to edit the current policy. Changes will be applied to all clients assigned to this policy.

NOTE: Refer to the ESET Remote Administrator User Guide for detailed information on policies.

Configure Background Scanning

In some cases, particularly when ESET Mail Security is installed in a clustered environment, background scanning can cause excess system load which can slow the reception and sending of email. If you notice that the transmission of email is slowed after installing ESET Mail Security we recommend that you disable Background scanning and create a new scheduled task to perform background scanning during non-work hours. To do so, follow the step-by-step instructions below:

1) Press **F5** to enter Advanced setup.

2) Expand **Server protection** > **Microsoft Exchange Server** > **Antivirus and antispyware** > **Microsoft Exchange Server** > **VSAPI x.x**.

3) Deselect the check box next to **Background scanning** and click **OK**. Email delivery speed should return to normal shortly.

4) Create a new scheduled task to perform the **Run mail server background scan** during non-work hours. For instructions to set up a scheduled background scan, see the Creating new tasks 89 section of this guide.

2.8 License

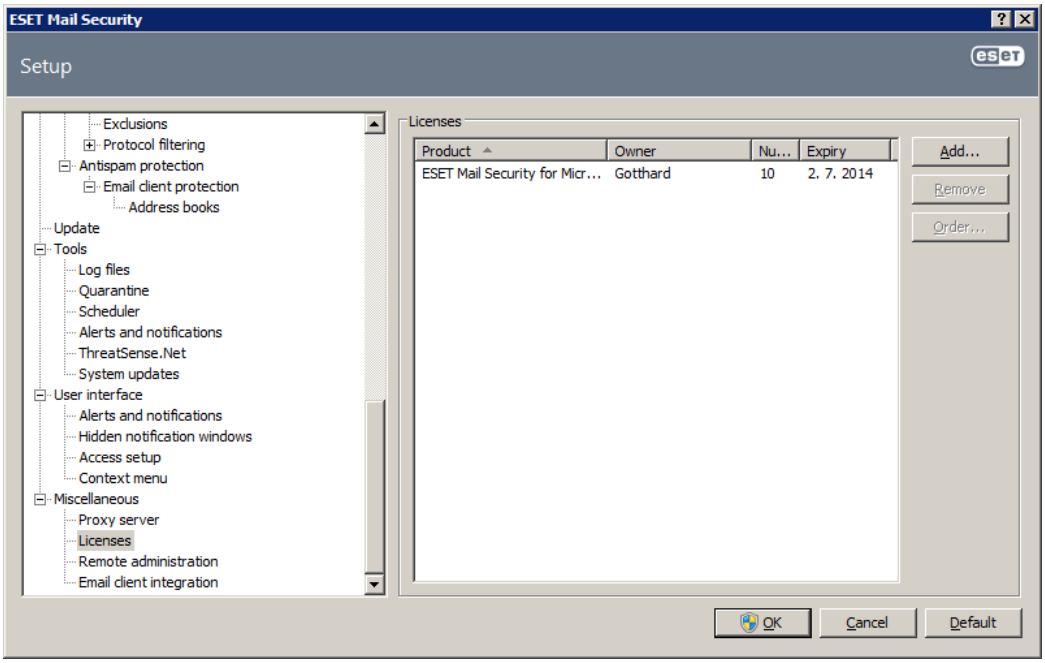
A very important step is to enter the license file for ESET Mail Security for Microsoft Exchange Server. Without it, email protection on the Microsoft Exchange Server will not work properly. If you do not add the license file during installation, you can do so later in the advanced settings, under **Miscellaneous > Licenses**.

ESET Mail Security allows you to use several licenses simultaneously by merging them, as is described in the following:

1) Two or more licenses of one customer (i.e. licenses assigned to the same customer name) are merged and the number of scanned mailboxes increases accordingly. The license manager will continue to display both licenses.

2) Two or more licenses of different customers are merged. This occurs exactly the same way as in the first scenario (point 1 above), with the only difference, that at least one of the licenses in question must have a special attribute. That attribute is required to merge licenses of different customers. If you are interested in using such a license, ask your local distributor to generate it for you.

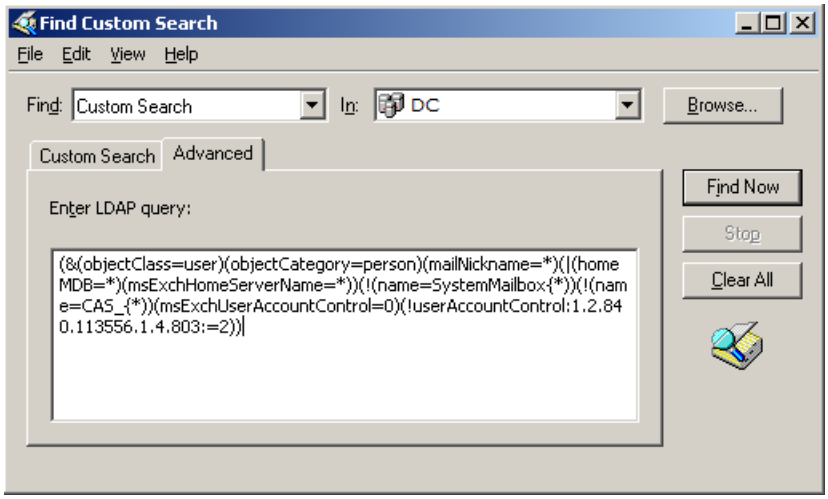
NOTE: Validity period of the newly created license is determined by the earliest expiration date from among its constituents.



ESET Mail Security for Microsoft Exchange Server (EMSX) compares the number of mailboxes for the active directory to your license count. Each Exchange server's active directory is checked to determine the total mailbox count. System mailboxes, deactivated mailboxes and email aliases are not tallied in the mailbox count. In a clustered environment, nodes with clustered mailbox role are not tallied in the mailbox count.

To determine how many Exchange enabled mailboxes you have, open **Active Directory users and computers** on the server. Right-click on the domain and click **Find...**. Then from the **Find** drop-down menu select **Custom search** and click the **Advanced** tab. Paste in the following Lightweight Directory Access Protocol (LDAP) query and click **Find Now**:

- `(&(objectClass=user)(objectCategory=person)(mailNickname=*)(|(homeMDB=*)(msExchHomeServerName=*))(!(name=SystemMailbox{*))(!(name=CAS_{*))(msExchUserAccountControl=0)(!userAccountControl:1.2.840.113556.1.4.803:=2))`



If the number of mailboxes in your active directory exceeds your license count a message will be entered into your Microsoft Exchange Server log reading, "Protection status changed due to exceeded number of mailboxes (count) covered by your license (count)." Your ESET Mail Security will also notify you by changing its **Protection status** to orange and displaying a message informing you that you have 42 days left before your protection will be disabled. If you receive this notification, please contact your sales representative to purchase additional licenses.

If the 42 days period has passed and you did not add the required licenses to cover the exceeding mailboxes, your **Protection status** will change to red. The message will inform you that your protection has been disabled. If you receive this notification, immediately contact your sales representative to purchase additional licenses.

2.9 Post-Installation Configuration

There are several options that have to be configured after the product installation.

Antispam protection setup

This section describes the settings, methods and techniques you can use to protect your network from spam. We recommend reading the following instructions carefully before choosing the most suitable combination of settings for your network.

Spam management

To ensure a high level of Antispam protection you must set actions to be performed on messages already marked as SPAM.

There are three options available:

1. **Deleting spam**
   The criteria for a message to be marked as SPAM by ESET Mail Security are set reasonably high, decreasing the chances of deleting legitimate email. The more specific the Antispam settings, the less likely it is to delete legitimate email. Advantages of this method include very low consumption of system resources and less administration. The drawback of this method is that if a legitimate email is deleted, it cannot be restored locally.

2. **Quarantine**
   This option excludes the risk of deleting legitimate email. Messages can be restored and resent to the original recipients immediately. The drawbacks of this method are higher consumption of system resources and additional time required for email quarantine maintenance. You can use two methods to quarantine email:

   A. Internal Exchange Server quarantine (applies only to Microsoft Exchange Server 2007/2010):
   - If you want to use the internal server quarantine, make sure the **Common message quarantine** field on the right pane in the advanced settings menu (under **Server protection** > **Message quarantine**) is left blank. Also make sure that the **Quarantine message to the mail server system quarantine** option is selected from the drop-down menu at the bottom. This method only works when the Exchange's internal quarantine exists. By default, this internal quarantine is not activated within Exchange. If you want to activate it, you need to open the Exchange Management Shell and type in following command:

   Set-ContentFilterConfig -QuarantineMailbox name@domain.com

   (replace name@domain.com by the actual mailbox you want Microsoft Exchange to use as an internal quarantine mailbox, e.g. exchangequarantine@company.com

   B. Custom quarantine mailbox:
   - If you type the desired mailbox in the **Common message quarantine** field, ESET Mail Security will move all new spam messages into your custom mailbox.

   For further details regarding Quarantine and different methods, see chapter Message quarantine 24.

3. **Forwarding spam**

   Spam will be forwarded along to its recipient. However, ESET Mail Security will fill in the relevant MIME header with the SCL value into each message. Based on the SCL value the relevant action will be executed by the Exchange server IMF (Intelligent Message Filtering).

Spam filtering

Greylisting

Greylisting is a method protecting users from spam using the following technique: Transport agent sends a "*temporarily reject*" SMTP return value (default is 451/4.7.1) for any email from a sender it does not recognize. A legitimate server will attempt to redeliver the message. Spammers typically do not attempt to redeliver messages, because they go through thousands of email addresses at a time and typically cannot spend extra time on resending.

When evaluating the message source, the method takes into account the configurations of the **Approved IP addresses** list, the **Ignored IP addresses** list, the **Safe Senders** and **Allow IP** lists on the Exchange server and the AntispamBypass settings for the recipient mailbox. Greylisting must be thoroughly configured, or else unwanted operational flaws (e.g. delays in legitimate message deliveries etc.) may occur. These negative effects recede continuously as this method fills the internal whitelist with trusted connections. If you are not familiar with this method, or if you consider its negative side-effect unacceptable, we recommend that you disable the method in the Advanced settings menu under **Antispam protection** > **Microsoft Exchange Server** > **Transport agent** > **Enable Greylisting.**

We recommend disabling greylisting if you intend to test the product's basic functionalities and do not want to configure the advanced features of the program.

NOTE: Greylisting is an additional layer of antispam protection and does not have any effect on the spam evaluation capabilities of the antispam module.

Configure Background Scanning

In some cases, particularly when ESET Mail Security is installed in a clustered environment, background scanning can cause excess system load which can slow the reception and sending of email. If you notice that the transmission of email is slowed after installing ESET Mail Security we recommend that you disable Background scanning and create a new scheduled task to perform background scanning during non-work hours. To do so, follow the step-by-step instructions below:

1) Press **F5** to enter Advanced setup.

2) Expand **Server protection** > **Microsoft Exchange Server** > **Antivirus and antispyware** > **Microsoft Exchange Server** > **VSAPI x.x**.

3) Deselect the check box next to **Background scanning** and click **OK**. Email delivery speed should return to normal shortly.

4) Create a new scheduled task to perform the **Run mail server background scan** during non-work hours. For instructions to set up a scheduled background scan, see the Creating new tasks 89 section of this guide.

Antivirus protection setup

Quarantine

Depending on the type of cleaning mode you are using, we recommend that you configure an action to be performed on infected (not cleaned) messages. This option can be set in the Advanced settings window **Server protection** > **Antivirus and antispyware** > **Microsoft Exchange Server** > **Transport agent**.

If the option to move messages into email quarantine is enabled, you need to configure the quarantine under **Server protection** > **Message quarantine** in the Advanced settings window.

Performance

If there are no other restrictions, our recommendation is to increase the number of ThreatSense scan engines in the Advanced settings window (F5) under **Computer protection** > **Antivirus and antispyware** > **Performance**, according to this formula: *number of ThreatSense scan engines = (number of physical CPUs x 2) + 1*. Also, the *number of scan threads* should be equal to the *number of ThreatSense scan engines*. You can configure the number of scan threads under **Server protection** > **Antivirus and antispyware** > **Microsoft Exchange Server** > **VSAPI** > **Performance**. Here is an example:

Let's say you have a server with 4 physical CPUs. For the best performance, according to formula above, you should have 9 scan threads and 9 scan engines.

NOTE: Acceptable value is 1-20, so the maximum number of ThreatSense scan engines you can use is 20. The change will be applied only after restart.

NOTE: We recommend that you set the number of scan threads equal to the number of ThreatSense scan engines used. It will have no effect on performance if you use more scan threads than scan engines.

NOTE: If you are using ESET Mail Security on a Windows Server that acts as a Terminal Server and do not want the ESET Mail Security GUI to start up every time a user logs in, see the Disable GUI on Terminal Server 116 chapter for specific steps to disable it.

3. ESET Mail Security - Microsoft Exchange Server protection

ESET Mail Security provides significant protection for your Microsoft Exchange Server. There are three essential types of protection: Antivirus, Antispam and the application of user-defined rules. ESET Mail Security protects from various types of malware content, including email attachments infected by worms or trojans, documents containing harmful scripts, phishing and spam. ESET Mail Security filters out the malicious content on the mail server level, before it arrives in the recipient's email client inbox. Following chapters describe all the options and settings available to you in order to fine-tune your Microsoft Exchange Server protection.

3.1 General settings

This section describes how to administer rules, log files, message quarantine and performance parameters.

3.1.1 Microsoft Exchange Server

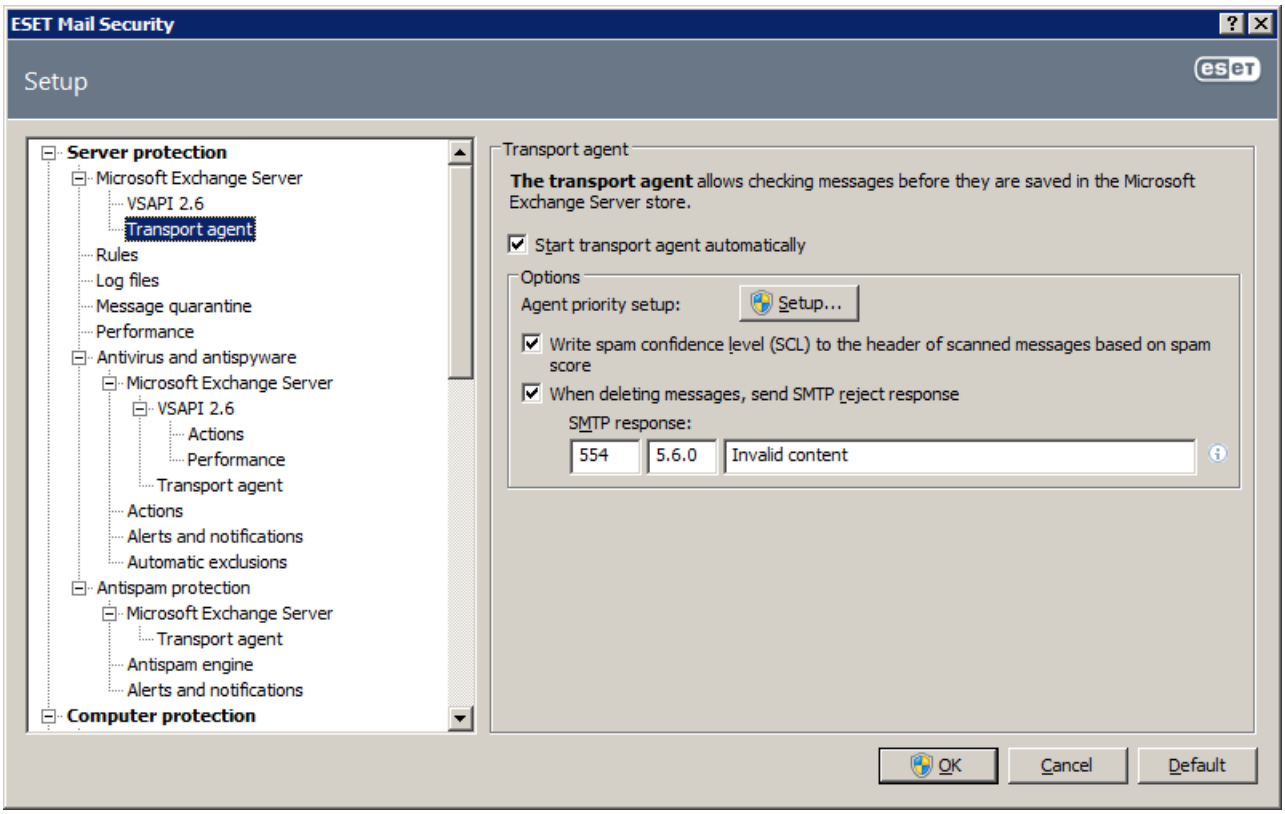
3.1.1.1 VSAPI (Virus-Scanning Application Programming Interface)

Microsoft Exchange Server provides a mechanism to make sure that every message component is scanned against the current virus signature database. If a message component is not scanned, its corresponding component is submitted to the scanner before the message is released to the client. Every supported version of Microsoft Exchange Server (2000/2003/2007/2010) offers a different version of VSAPI.

Use the checkbox to enable/disable the automatic startup of the VSAPI version used by your Exchange server.

3.1.1.2 Transport Agent

In this section, you can configure the transport agent to automatically start and set the agent loading priority. On Microsoft Exchange Server 2007 and later, it is only possible to install a transport agent if the server is in one of two roles: *Edge Transport* or *Hub Transport*.



NOTE: The Transport agent is not available in Microsoft Exchange Server 5.5 (VSAPI 1.0).

In the **Agent priority setup** menu, you can set the priority of ESET Mail Security agents. The agent priority number range depends on the version of Microsoft Exchange Server (the lower the number, the higher the priority).

Write spam confidence level (SCL) to the header of scanned messages based on spam score – SCL is a

normalized value assigned to a message that indicates the likelihood of the message being spam (based on the characteristics of the message header, its subject, content, etc.). A rating of 0 indicates that the message is highly unlikely to be spam, while a rating of 9 indicates that the message is very likely spam. SCL values can be processed further by the Microsoft Exchange Server's Intelligent Message Filter (or Content Filter Agent). For additional information, please refer to the Microsoft Exchange Server documentation.

The **When deleting messages, send SMTP reject response** option:

- If unchecked, the server sends an OK SMTP response to the sender's Mail Transfer Agent (MTA) in the format '250 2.5.0 – Requested mail action okay, completed' and then performs a silent drop.
- If checked, an SMTP reject response is sent back to the sender's MTA. You can type a response message in the following format:

Primary response code	Complementary status code	Description
250	2.5.0	Requested mail action okay, completed
451	4.5.1	Requested action aborted: local error in processing
550	5.5.0	Requested action not taken: mailbox unavailable

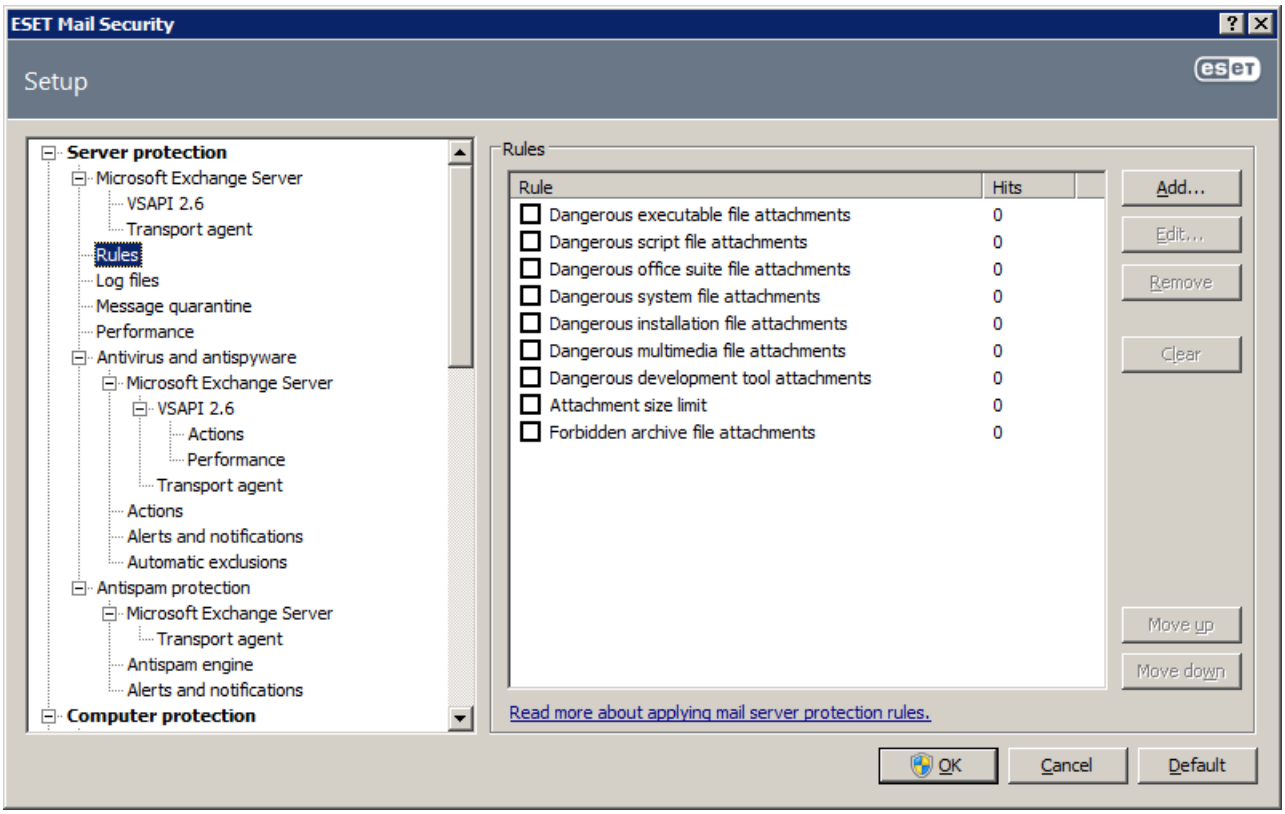
Warning: Incorrect syntax of the SMTP response codes can lead to program components malfunctioning and a decrease in

NOTE: You can also use system variables when configuring SMTP Reject Responses.

3.1.2 Rules

The **Rules** menu item allows administrators to manually define email filtering conditions and actions to take with filtered emails. The rules are applied according to a set of combined conditions. Multiple conditions are combined with the logical operator AND, applying the rule only if all the conditions are met. The **Number** column (next to each rule name) displays the number of times the rule was successfully applied.

The rules are checked against a message when it is processed by the transport agent (TA) or VSAPI. When both the TA and VSAPI are enabled and the message matches the rule conditions, the rule counter may increase by 2 or more. This is because the VSAPI accesses each part of the message individually (body, attachment) meaning the rules are consequently applied to each part individually. Rules are also applied during background scanning (e.g. repeated mailbox-store scan after a virus signature database update), which can increase the rule counter.



- **Add...** - adds a new rule
- **Edit...** - modifies an existing rule
- **Remove** - removes selected rule
- **Clear** - clears the rule counter (the Hits column)
- **Move up** - moves selected rule up in the list
- **Move down** - moves selected rule down in the list

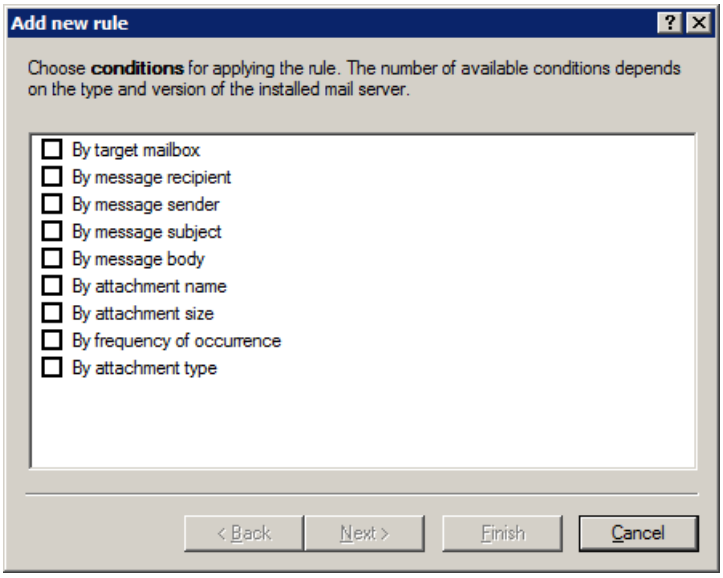
Unchecking a check box (to the left of each rule name) deactivates current rule. This allows for the rule to be reactivated again if needed.

NOTE: You can also use system variables (e.g., *%PATHEXT%*) when configuring Rules.

NOTE: If a new rule has been added or an existing rule has been modified, a message rescan will automatically start using the new/modified rules.

3.1.2.1 Adding new rules

This wizard guides you through adding user-specified rules with combined conditions.


Add new rule
Choose conditions for applying the rule. The number of available conditions depends on the type and version of the installed mail server.
By target mailbox
By message recipient
By message sender
By message subject
By message body
By attachment name
By attachment size
By frequency of occurrence
By attachment type
< Back
Next >
Finish
Cancel

NOTE: Not all of the conditions are applicable when the message is scanned by the transport agent.

- **By target mailbox** applies to the name of a mailbox (VSAPI)
- **By message recipient** applies to a message sent to a specified recipient (VSAPI + TA)
- **By message sender** applies to a message sent by a specified sender (VSAPI + TA)
- **By message subject** applies to a message with a specified subject line (VSAPI + TA)
- **By message body** applies to a message with specific text in the message body (VSAPI)
- **By attachment name** applies to a message with a specific attachment name (VSAPI in Exchange 2000 and 2003, VSAPI + TA in Exchange 2007 and 2010)
- **By attachment size** applies to a message with an attachment exceeding a defined size (VSAPI in Exchange 2000 and 2003, VSAPI + TA in Exchange 2007 and 2010)
- **By frequency of occurrence** applies to objects (email body or attachment) where the number of occurrences within the specified time interval exceeds the specified number (VSAPI). This is particularly useful if you are constantly spammed with emails with the same email body or the same attachment
- **By attachment type** applies to a message with an attachment of specified file type (actual file type is detected by its contents, regardless of file extension) (VSAPI)

When specifying the conditions above (except the **By attachment size** condition), it is sufficient to fill in only part of a phrase as long as the **Match whole words** option is not selected. Values are not case-sensitive, unless the **Match case** option is selected. If you are using values other than alphanumerical characters, use parentheses and quotes. You can also create conditions using the logical operators AND, OR and NOT.

NOTE: The list of available rules depends on installed version of Microsoft Exchange Server.

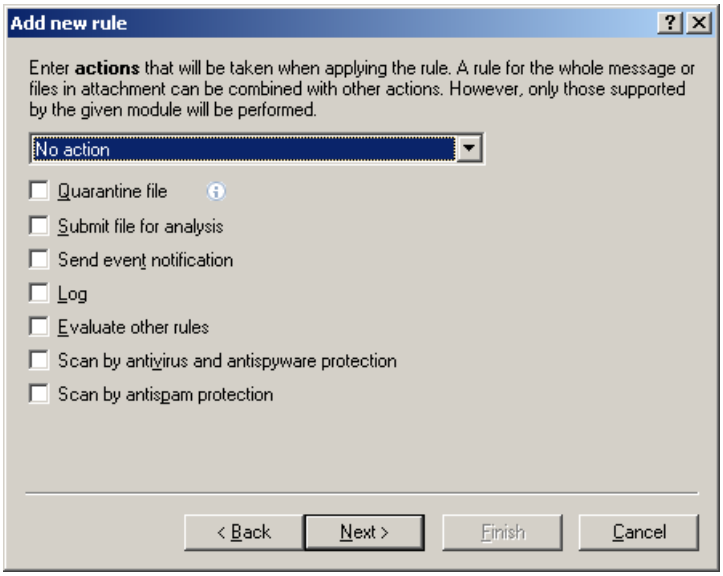
NOTE: Microsoft Exchange Server 2000 (VSAPI 2.0) only evaluates displayed sender/recipient name and not the email address. Email addresses are evaluated starting with Microsoft Exchange Server 2003 (VSAPI 2.5) and higher.

Examples of entering conditions:

By target mailbox:	smith
By email sender:	smith@mail.com
By email recipient:	"J.Smith" or "smith@mail.com"
By email subject:	" "
By attachment name:	".com" OR ".exe"
By email body:	("free" OR "lottery") AND ("win" OR "buy")

3.1.2.2 Actions taken when applying rules

This section allows you to select actions to take with messages and/or attachments matching conditions defined in rules. You can take no action, mark the message as if it contained a threat/spam or delete the whole message. When a message or its attachment matches the rule conditions, it is not scanned by the antivirus or antispam modules by default, unless scanning is enabled explicitly by selecting the respective check boxes at the bottom (the action taken then depends on the antivirus/antispam settings).


Add new rule
Enter actions that will be taken when applying the rule. A rule for the whole message or files in attachment can be combined with other actions. However, only those supported by the given module will be performed.
No action
Quarantine file
Submit file for analysis
Send event notification
Log
Evaluate other rules
Scan by antivirus and antispyware protection
Scan by antispam protection
< Back
Next >
Finish
Cancel

- **No action** – no action will be taken with the message
- **Take action for uncleaned threat** - the message will be marked as if it contained an uncleaned threat (regardless of whether it contained the threat or not)
- **Take action for unsolicited email** - the message will be marked as if it were spam (regardless of whether it is spam or not). This option will only work if antispam protection 35 is enabled and the action is being performed on transport agent level. Otherwise this action will not be performed
- **Delete message** – removes the entire message with content that meets the conditions, however this action only works on VSAPI 2.5 and newer (VSAPI 2.0 and older cannot perform this action)

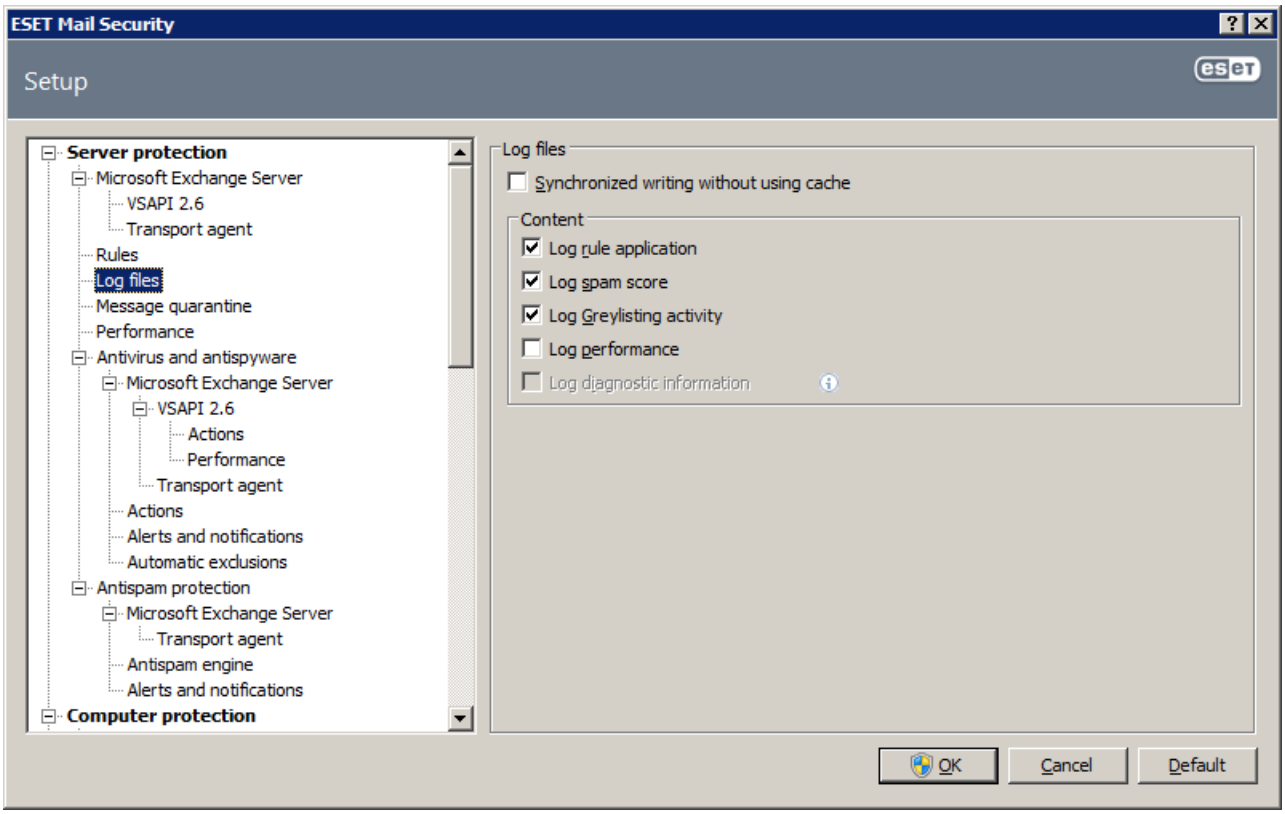
- **Quarantine file** - attached file(s) that meet the rules criteria will be put into file quarantine of ESET Mail Security, do not confuse this with the mail quarantine (for more information about mail quarantine see Message quarantine 24)
- **Submit file for analysis** - sends suspicious attachments to the ESET lab for analysis
- **Send event notification** - sends a notification to the administrator (based on settings in **Tools** > **Alerts and notifications**)
- **Log** - writes information about the applied rule to the program log
- **Evaluate other rules** - allows the evaluation of other rules, enabling the user to define multiple sets of conditions and multiple actions to take, given the conditions
- **Scan by antivirus and antispyware protection** - scans the message and its attachments for threats
- **Scan by antispam protection** - scans the message for spam

NOTE: This option is available only in Microsoft Exchange Server 2000 and later with the transport agent turned on.

The last step in the new rule creation wizard is to name each created rule. You can also add a **Rule comment**. This information will be stored in the Microsoft Exchange Server log.

3.1.3 Log files

Log files settings let you choose how the log file will be assembled. More detailed protocol can contain more information, but it may slow down server's performance.

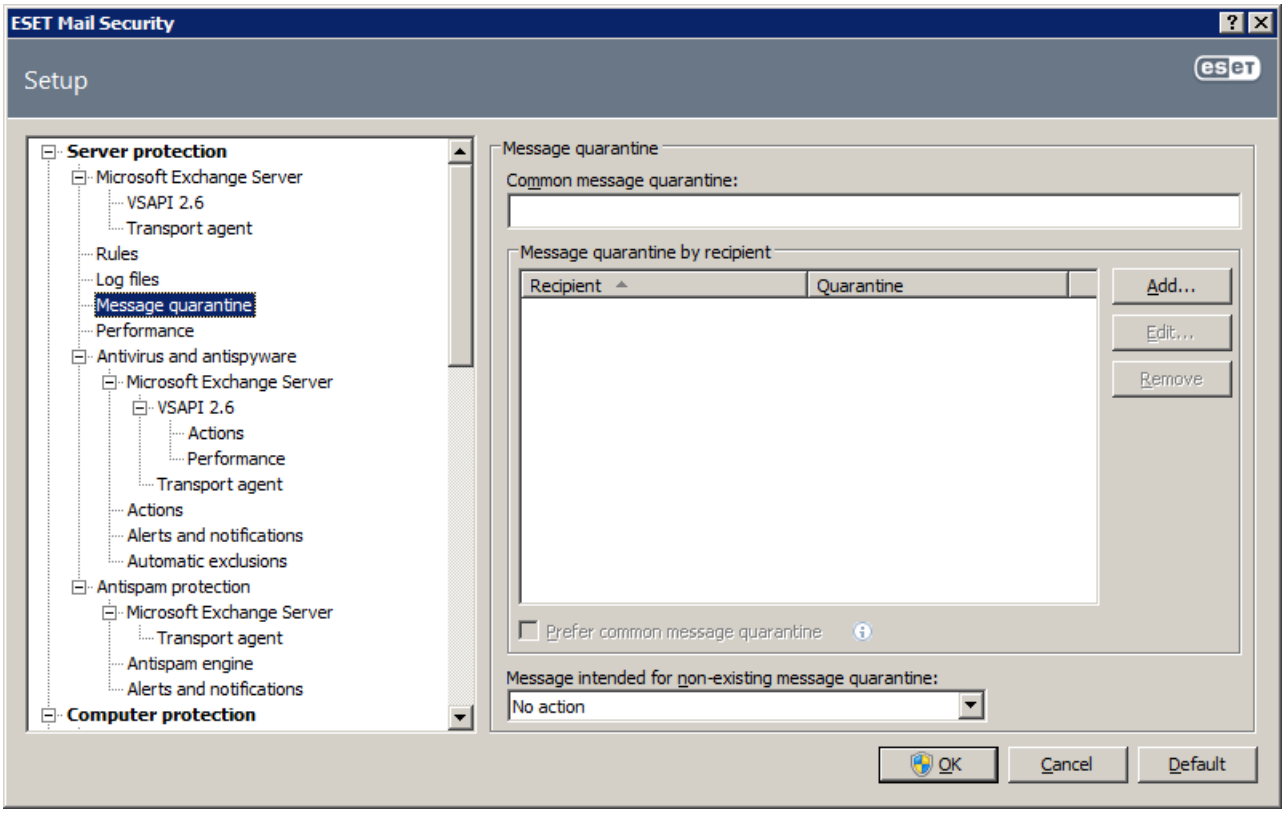


If **Synchronized writing without using cache** is enabled, all the log entries will be immediately written in the log file without being stored in the log cache. By default, ESET Mail Security components running in Microsoft Exchange Server store log messages in their internal cache and send them to the application log at periodic time intervals to preserve performance. In this case, however, the diagnostic entries in the log might not be in the proper order. We recommend keeping this setting turned off unless it is necessary for diagnostics. You can specify the type of information stored in the log files in the **Content** menu.

- **Log rule application** - when this option is enabled, ESET Mail Security writes the name of all activated rules into the log file.
- **Log spam score** - use this option to have spam related activity written to Antispam log 92. When the mail server receives a SPAM message, information about this is written into the log providing details such as the Time/Date, Sender, Recipient, Subject, SPAM Score, Reason and Action. This is useful when you need to track down what SPAM messages were received, when and what action was taken.
- **Log Greylisting activity** - enable this option if you want to have Greylisting related activity written into the Greylisting log 92. It provides information such as Time/Date, HELO Domain, IP address, Sender, Recipient, Action, etc.
  NOTE: This option works only when Greylisting is enabled within Transport agent 36 options under **Server protection** > **Antispam protection** > **Microsoft Exchange Server** > **Transport agent** in the advanced setup tree (F5).
- **Log performance** - logs information about the time interval of a performed task, size of the scanned object, transfer rate (kb/s) and performance rating.
- **Log diagnostic information** - logs diagnostic information needed for fine-tuning of the program to the protocol; this option is mostly for debugging and identifying problems. Having this option turned on is not recommended. To see diagnostic information provided by this function, you will have to set the Minimum logging verbosity to **Diagnostic records** in the **Tools** > **Log files** > **Minimum logging verbosity** setting.

3.1.4 Message quarantine

The **Message quarantine** is a special mailbox defined by the system administrator to store potentially infected messages and SPAM. Messages stored in quarantine can be analyzed or cleaned later using a newer virus signature database.



There are two types of message quarantine systems that can be used.

One option is to use the Microsoft Exchange quarantine system (this applies only to Microsoft Exchange Server 2007/2010). In this case, the Exchange's internal mechanism is used to store potentially infected messages and SPAM. Additionally, you can add a separate quarantine mailbox (or number of mailboxes) for specific recipients if needed. This means that potentially infected messages, which were originally sent to a specific recipient, will be delivered to separate quarantine mailbox instead of being delivered to Exchange's internal quarantine mailbox. This might be useful in some cases to keep potentially infected messages and SPAM more organized.

Other option is to use **Common message quarantine**. If you are using an earlier version of Microsoft Exchange Server (5.5, 2000 or 2003), then you simply specify **Common message quarantine**, which is a mailbox that will be used to store potentially infected messages. In this case, Exchange's internal quarantine system is not used. Instead, a mailbox specified by the system administrator is used for this purpose. As with the first option, you can add a separate quarantine mailbox (or number of mailboxes) for specific recipients. The result is that potentially infected messages are delivered to a separate mailbox instead of being delivered to common message quarantine.

- **Common message quarantine** - you can specify common message quarantine address here (e.g. main_quarantine@company.com), or you can use the Microsoft Exchange Server 2007/2010 internal quarantine system instead by leaving this field blank and choosing **Quarantine message to the mail server system quarantine** (provided that the Exchange quarantine exists in your environment) from the drop-down menu at the bottom. Emails are then delivered to quarantine by Exchange's internal mechanism using its own settings. **NOTE**: By default, this internal quarantine is not activated within Exchange. If you want to activate it, you need to open Exchange Management Shell and type in following command:

  Set-ContentFilterConfig -QuarantineMailbox name@domain.com

  (replace name@domain.com by the actual mailbox you want Microsoft Exchange to use as an internal quarantine mailbox, e.g. exchangequarantine@company.com)

- **Message quarantine by recipient** - by using this option, you can define message quarantine mailboxes for multiple recipients. Every quarantine rule can be enabled or disabled by checking or unchecking the check box in its row.

  Add... - you can add a new quarantine rule by entering the desired recipient's email address and the quarantine email address to which mail will be forwarded

  Edit... - edit a selected quarantine rule

  Remove - remove a selected quarantine rule

  Prefer common message quarantine - when enabled, a message will be delivered to the specified common quarantine if more than one quarantine rule is met (e.g., if a message has multiple recipients and some of them are defined in multiple quarantine rules)

- **Message intended for non-existing message quarantine** (if you did not specify a common message quarantine, you have following options as to what action will be taken on possibly infected messages and SPAM)

  No action - a message will be processed in a standard way - delivered to the recipient (not recommended)
  Delete message - a message will be deleted if it is addressed to a recipient with no existing quarantine rule and a common message quarantine is not specified, this means that all possibly infected messages and SPAM will be automatically deleted without being stored anywhere
  Quarantine message to the mail server system quarantine - a message will be delivered to and stored in the Exchange's internal system quarantine (not available for Microsoft Exchange Server 2003 and earlier)

NOTE: You can also use system variables (e.g., *%USERNAME%*) when configuring Message Quarantine settings.

3.1.4.1 Adding a new quarantine rule

Enter the Recipient's email address and the Quarantine email address in the appropriate fields.

If you want to delete an email message addressed to a recipient who does not have a quarantine rule applied, you can select **Delete message** from the **Message intended for non-existing message quarantine** drop-down menu.

3.1.5 Performance

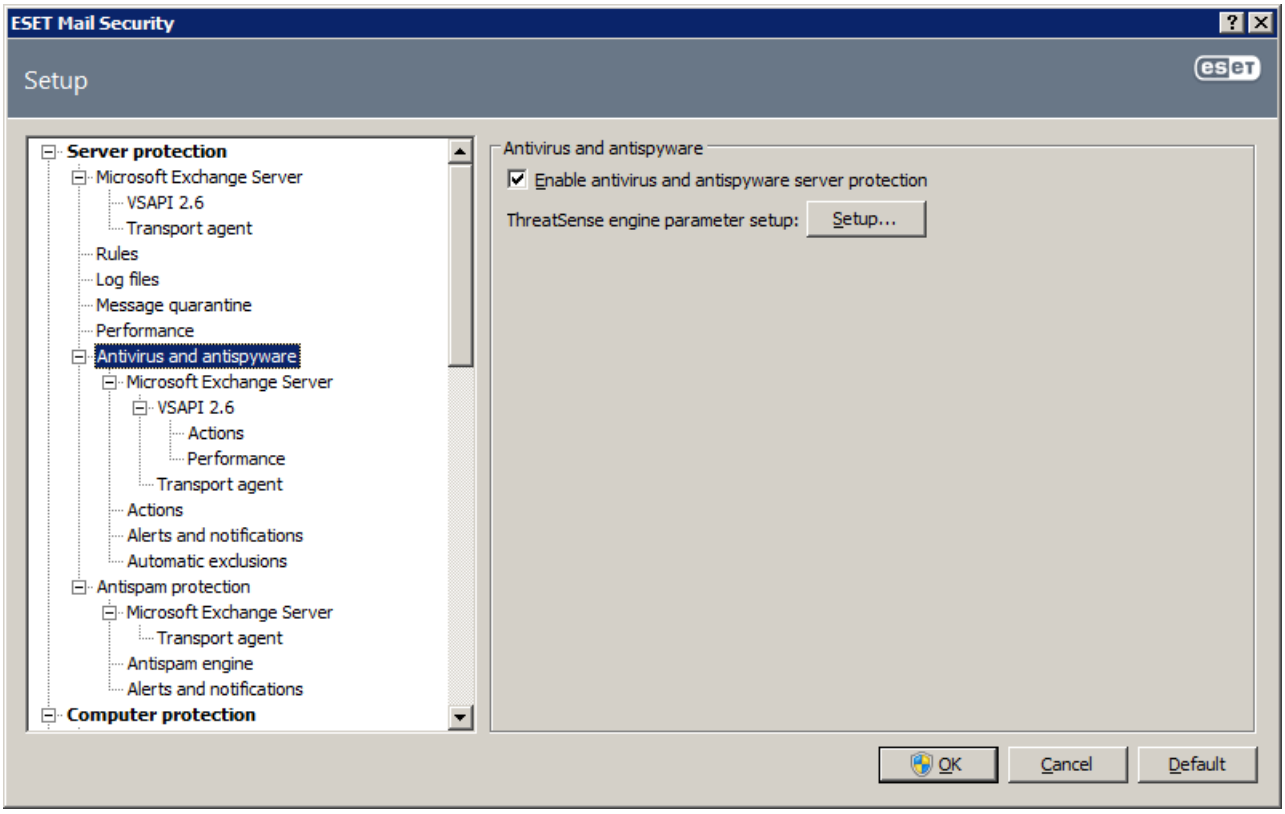
In this section you can define a folder to store temporary files in to improve program performance. If no folder is specified, ESET Mail Security will create temporary files in the system's temporary folder.

NOTE: In order to reduce the potential I/O and fragmentation impact, we recommend placing the Temporary folder on a different hard drive than the one on which Microsoft Exchange Server is installed. We strongly recommend that you avoid assigning the Temporary folder to removable media such as floppy disk, USB, DVD, etc.

NOTE: You can use system variables (e.g. *%SystemRoot%\TEMP*) when configuring Performance settings.

3.2 Antivirus and antispyware settings

You can enable antivirus and antispyware mail server protection by selecting the **Enable antivirus and antispyware server protection** option. Note that antivirus and antispyware protection is turned on automatically after every restart of the service/computer. ThreatSense engine parameter setup is accessible by clicking on the **Setup...** button.



3.2.1 Microsoft Exchange Server

When it comes to antivirus and antispyware protection, ESET Mail Security for Microsoft Exchange Server uses two types of scanning. One type scans messages via VSAPI and the other uses Transport Agent.

- Protection using VSAPI 27 scans messages directly within the Exchange server store.
- Transport Agent 32 protection scans SMTP traffic instead of the Exchange server store itself. If this type of protection is enabled, it means that all the messages and their components are being scanned during transportation, even before it reaches the Exchange server store or before it is sent out via SMTP. SMTP server-level filtering is secured by a specialized plugin. In Microsoft Exchange Server 2000 and 2003, the plugin in question (Event Sink) is registered on the SMTP server as a part of Internet Information Services (IIS). In Microsoft Exchange Server 2007/2010, the plugin is registered as a transport agent on the Edge or the Hub roles of the Microsoft Exchange Server.

NOTE: Transport agent is not available in Microsoft Exchange Server 5.5, however it is available in all newer Microsoft Exchange Server versions (from version 2000 onwards).

You can have VSAPI and Transport agent antivirus and antispyware protection working at the same time (this is the default and recommended configuration). Alternatively, you can choose to use only one type of protection (either VSAPI or Transport agent). They can be enabled or disabled independently of each other. We recommend using both types to ensure maximum antivirus and antispyware protection. We do not recommend having both disabled.

3.2.1.1 Virus-Scanning Application Programming Interface (VSAPI)

Microsoft Exchange Server provides a mechanism to make sure that every message component is scanned against the current virus signature database. If a message was not previously scanned, its corresponding components are submitted to the scanner before the message is released to the client. Every supported version of Microsoft Exchange Server (5.5/2000/2003/2007/2010) offers a different version of VSAPI.

3.2.1.1.1 Microsoft Exchange Server 5.5 (VSAPI 1.0)

This version of Microsoft Exchange Server includes VSAPI version 1.0.

If the **Background scanning** option is enabled, it allows for scanning of all messages in the system background. Microsoft Exchange Server decides whether a background scan will run or not, based on various factors, such as the current system load, the number of active users, etc. Microsoft Exchange Server keeps a record of scanned messages and the virus signature database version used. If you are opening a message that has not been scanned by the most current virus signature database, Microsoft Exchange Server sends the message to ESET Mail Security to be scanned before opening the message in your email client.

Since background scanning can affect system load (scanning is performed after each virus signature database update), we recommend using scheduled scanning outside working hours. Scheduled background scanning can be configured via a special task in the Scheduler/Planner. When you schedule a Background scanning task you can set the launch time, the number of repetitions and other parameters available in the Scheduler/Planner. After the task has been scheduled, it will appear in the list of scheduled tasks and, as with the other tasks, you can modify its parameters, delete it or temporarily deactivate the task.

3.2.1.1.1.1 Actions

In this section you can specify the actions to be performed when a message and/or attachment is evaluated as infected.

The **Action to take if cleaning not possible** field allows you to **Block** infected content, **Delete** the message or take **No action** on the infected content of the message. This action will be applied only if the automatic cleaning (defined in **ThreatSense engine parameter setup** > Cleaning 74) did not clean the message.

The **Deletion** field allows you to set **Attachment deletion method** to either of these options:

- **Truncate file to zero length** – ESET Mail Security truncates the attachment to zero size and lets the recipient see the attachment file name and type
- **Replace attachment with action information** – ESET Mail Security replaces the infected file with a virus protocol or rule description

By clicking the **Rescan** button you will run another scan on messages and files that have already been scanned before.

3.2.1.1.1.2 Performance

During a scan, Microsoft Exchange Server allows you to limit a time for opening message attachments. This time is set in the **Response time limit (ms)** field and represents the period after which the client will retry accessing the file that had previously been inaccessible due to scanning.

3.2.1.1.2 Microsoft Exchange Server 2000 (VSAPI 2.0)

This version of Microsoft Exchange Server includes VSAPI version 2.0.

If you uncheck the **Enable antivirus and antispyware VSAPI 2.0 protection** option, the ESET Mail Security plug-in for Exchange server will not get unloaded from the Microsoft Exchange server process. It will only pass through the messages without scanning for viruses. The messages however, will still be scanned for spam 36 and the rules 20 will be applied.

If the **Proactive scanning** option is enabled, new inbound messages will be scanned in the same order in which they were received. If this option is enabled and a user opens a message that has not been scanned yet, this message will be scanned before the other messages in the queue.

The **Background scanning** option allows scanning of all messages in the system background. Microsoft Exchange

Server decides whether a background scan will run or not, based on various factors, such as the current system load, the number of active users, etc. Microsoft Exchange Server keeps a record of scanned messages and the virus signature database version used. If you are opening a message that has not been scanned by the most current virus signature database, Microsoft Exchange Server sends the message to ESET Mail Security to be scanned before opening the message in your email client.

Since background scanning can affect system load (scanning is performed after each virus signature database update), we recommend using scheduled scanning outside working hours. Scheduled background scanning can be configured via a special task in the Scheduler/Planner. When you schedule a Background scanning task you can set the launch time, the number of repetitions and other parameters available in the Scheduler/Planner. After the task has been scheduled, it will appear in the list of scheduled tasks and as with the other tasks, you can modify its parameters, delete it or temporarily deactivate the task.

If you want to scan plain text messages, select the **Scan plain text message bodies** option.

Enabling the **Scan RTF message bodies** option activates scanning of RTF message bodies. The RTF message bodies may contain macro viruses.

3.2.1.1.2.1 Actions

In this section you can specify the actions to be performed when a message and/or attachment is evaluated as infected.

The **Action to take if cleaning not possible** field allows you to **Block** infected content, **Delete** the message or take **No action** on the infected content of the message. This action will be applied only if the automatic cleaning (defined in **ThreatSense engine parameter setup >** Cleaning 74) did not clean the message.

The **Deletion** option allows you set **Message deletion method** and **Attachment deletion method**.

You can set **Message deletion method** to:

- **Delete message body** – delete the body of the infected message; the recipient will receive an empty message and any non-infected attachments
- **Rewrite message body with action information** – rewrite the body of the infected message with information about performed actions

You can set **Attachment deletion method** to:

- **Truncate file to zero length** – ESET Mail Security truncates the attachment to zero size and lets the recipient see the attachment file name and type
- **Replace attachment with action information** – ESET Mail Security replaces the infected file with a virus protocol or rule description

By clicking the **Rescan** button you will run another scan on messages and files that have already been scanned before.

3.2.1.1.2.2 Performance

In this section you can set the number of independent scan threads used at a single time. More threads on multiprocessor machines can increase the scan rate. For the best program performance we advise using an equal number of ThreatSense scan engines and scan threads.

The **Response time limit (sec.)** allows you to set the maximum amount of time a thread waits for a message scan to complete. If the scan is not finished within this time limit, Microsoft Exchange Server will deny the client access to the email. Scanning will not be interrupted and, after it is finished, every other attempt to access the file will be successful.

TIP: To determine the **Number of scan threads** the Microsoft Exchange Server provider recommends, use the following formula: [number of physical processors] x 2 + 1.

NOTE: Performance is not improved significantly if there are more ThreatSense scanning engines than scanning threads.

3.2.1.1.3 Microsoft Exchange Server 2003 (VSAPI 2.5)

This version of Microsoft Exchange Server includes VSAPI version 2.5.

If you uncheck the **Enable antivirus and antispyware VSAPI 2.5 protection** option, the ESET Mail Security plug-in for Exchange server will not get unloaded from the Microsoft Exchange server process. It will only pass through the messages without scanning for viruses. The messages however, will still be scanned for spam 36 and the rules 20 will be applied.

If the **Proactive scanning** option is enabled, new inbound messages will be scanned in the same order in which they were received. If this option is enabled and a user opens a message that has not been scanned yet, this message will be scanned before the other messages in the queue.

The **Background scanning** option allows scanning of all messages in the system background. Microsoft Exchange Server decides whether a background scan will run or not, based on various factors, such as the current system load, the number of active users, etc. Microsoft Exchange Server keeps a record of scanned messages and the virus signature database version used. If you are opening a message that has not been scanned by the most current virus signature database, Microsoft Exchange Server sends the message to ESET Mail Security to be scanned before opening the message in your email client.

Since background scanning can affect system load (scanning is performed after each virus signature database update), we recommend using scheduled scanning outside working hours. Scheduled background scanning can be configured via a special task in the Scheduler/Planner. When you schedule a Background scanning task you can set the launch time, the number of repetitions and other parameters available in the Scheduler/Planner. After the task has been scheduled, it will appear in the list of scheduled tasks and as with the other tasks, you can modify its parameters, delete it or temporarily deactivate the task.

Enabling the **Scan RTF message bodies** option activates scanning of RTF message bodies. The RTF message bodies may contain macro viruses.

The **Scan transported messages** option enables scanning of messages which are not stored on the local Microsoft Exchange Server and are being delivered to other email servers through the local Microsoft Exchange Server. The Microsoft Exchange Server can be configured as a gateway which then passes messages to other email servers. If scanning for transported messages is enabled, ESET Mail Security also scans these messages. This option is only available when the transport agent is disabled.

NOTE: Plain text email bodies are not scanned by VSAPI.

3.2.1.1.3.1 Actions

In this section you can specify the actions to be performed when a message and/or attachment is evaluated as infected.

The **Action to take if cleaning not possible** field allows you to **Block** infected content, **Delete** infected content of the message, **Delete whole message** including infected content or take **No action**. This action will be applied only if the automatic cleaning (defined in **ThreatSense engine parameter setup >** Cleaning 74) did not clean the message.

The **Deletion** option allows you set **Message deletion method** and **Attachment deletion method**.

You can set **Message deletion method** to:

- **Delete message body** – delete the body of the infected message; the recipient will receive an empty message and any non-infected attachments
- **Rewrite message body with action information** – rewrite the body of the infected message with information about performed actions
- **Delete whole message** – delete the entire message, including attachments; you can set what action should be performed when deleting attachments

You can set **Attachment deletion method** to:

- **Truncate file to zero length** – ESET Mail Security truncates the attachment to zero size and lets the recipient see the attachment file name and type
- **Replace attachment with action information** – ESET Mail Security replaces the infected file with a virus protocol or rule description
- **Delete whole message** – delete the entire message, including attachments; you can set what action should be performed when deleting attachments

By clicking the **Rescan** button you will run another scan on messages and files that have already been scanned before.

3.2.1.1.3.2 Performance

In this section you can set the number of independent scan threads used at a single time. More threads on multiprocessor machines can increase the scan rate. For the best program performance we advise using an equal number of ThreatSense scan engines and scan threads.

The **Response time limit (sec.)** allows you to set the maximum amount of time a thread waits for a message scan to complete. If the scan is not finished within this time limit, Microsoft Exchange Server will deny the client access to the email. Scanning will not be interrupted and, after it is finished, every other attempt to access the file will be successful.

TIP: To determine the **Number of scan threads** the Microsoft Exchange Server provider recommends, use the following formula: [number of physical processors] x 2 + 1.

NOTE: Performance is not improved significantly if there are more ThreatSense scanning engines than scanning threads.

3.2.1.1.4 Microsoft Exchange Server 2007/2010 (VSAPI 2.6)

This version of Microsoft Exchange Server includes VSAPI version 2.6.

If you uncheck the **Enable antivirus and antispyware protection VSAPI 2.6** option, the ESET Mail Security plug-in for Exchange server will not get unloaded from the Microsoft Exchange server process. It will only pass through the messages without scanning for viruses. The messages however, will still be scanned for spam 36 and the rules 20 will be applied.

If the **Proactive scanning** option is enabled, new inbound messages will be scanned in the same order in which they were received. If this option is enabled and a user opens a message that has not been scanned yet, this message will be scanned before the other messages in the queue.

The **Background scanning** option allows scanning of all messages in the system background. Microsoft Exchange Server decides whether a background scan will run or not, based on various factors, such as the current system load, the number of active users, etc. Microsoft Exchange Server keeps a record of scanned messages and the virus signature database version used. If you are opening a message that has not been scanned by the most current virus signature database, Microsoft Exchange Server sends the message to ESET Mail Security to be scanned before opening the message in your email client. You can choose to **Scan only messages with attachment** and filter based on time received with the following **Scan level** options:

- **All messages**
- **Messages received within last year**
- **Messages received within last 6 months**
- **Messages received within last 3 months**
- **Messages received within last months**
- **Messages received within last week**

Since background scanning can affect system load (scanning is performed after each virus signature database update), we recommend using scheduled scanning outside working hours. Scheduled background scanning can be configured via a special task in the Scheduler/Planner. When you schedule a Background scanning task you can set the launch time, the number of repetitions and other parameters available in the Scheduler/Planner. After the task has been scheduled, it will appear in the list of scheduled tasks and as with the other tasks, you can modify its parameters, delete it or temporarily deactivate the task.

Enabling the **Scan RTF message bodies** option activates scanning of RTF message bodies. RTF message bodies may contain macro viruses.

NOTE: Plain text email bodies are not scanned by VSAPI.

3.2.1.1.4.1 Actions

In this section you can specify the actions to be performed when a message and/or attachment is evaluated as infected.

The **Action to take if cleaning not possible** field allows you to **Block** infected content, **Delete object** - infected content of the message, **Delete whole message** or take **No action**. This action will be applied only if the automatic cleaning (defined in **ThreatSense engine parameter setup** > Cleaning 74) did not clean the message.

As described above, you can set **Action to take if cleaning not possible** to:

- **No action** – take no action on the infected content of the message
- **Block** – block the message before it is received in Microsoft Exchange Server storage
- **Delete object** – delete the infected content of the message
- **Delete whole message** – delete the entire message, including its infected content

The **Deletion** option allows you set **Message body deletion method** and **Attachment deletion method**.

You can set **Message body deletion method** to:

- **Delete message body** – delete the body of the infected message; the recipient will receive an empty message and any non-infected attachments
- **Rewrite message body with action information** – rewrite the body of the infected message with information about performed actions
- **Delete whole message** – delete the entire message, including attachments; you can set what action should be performed when deleting attachments

You can set **Attachment deletion method** to:

- **Truncate file to zero length** – ESET Mail Security truncates the attachment to zero size and lets the recipient see the attachment file name and type
- **Replace attachment with action information** – ESET Mail Security replaces the infected file with a virus protocol or rule description
- **Delete whole message** – delete the attachment

If the **Use VSAPI Quarantine** option is enabled, infected messages will be stored in the email server quarantine. Please note that this is the server's managed VASPI quarantine (not the client's quarantine or the quarantine mailbox). Infected messages stored in mail server quarantine are inaccessible until they are cleaned with the latest virus signature database.

By clicking the **Rescan** button you will run another scan on messages and files that have already been scanned before.

3.2.1.1.4.2 Performance

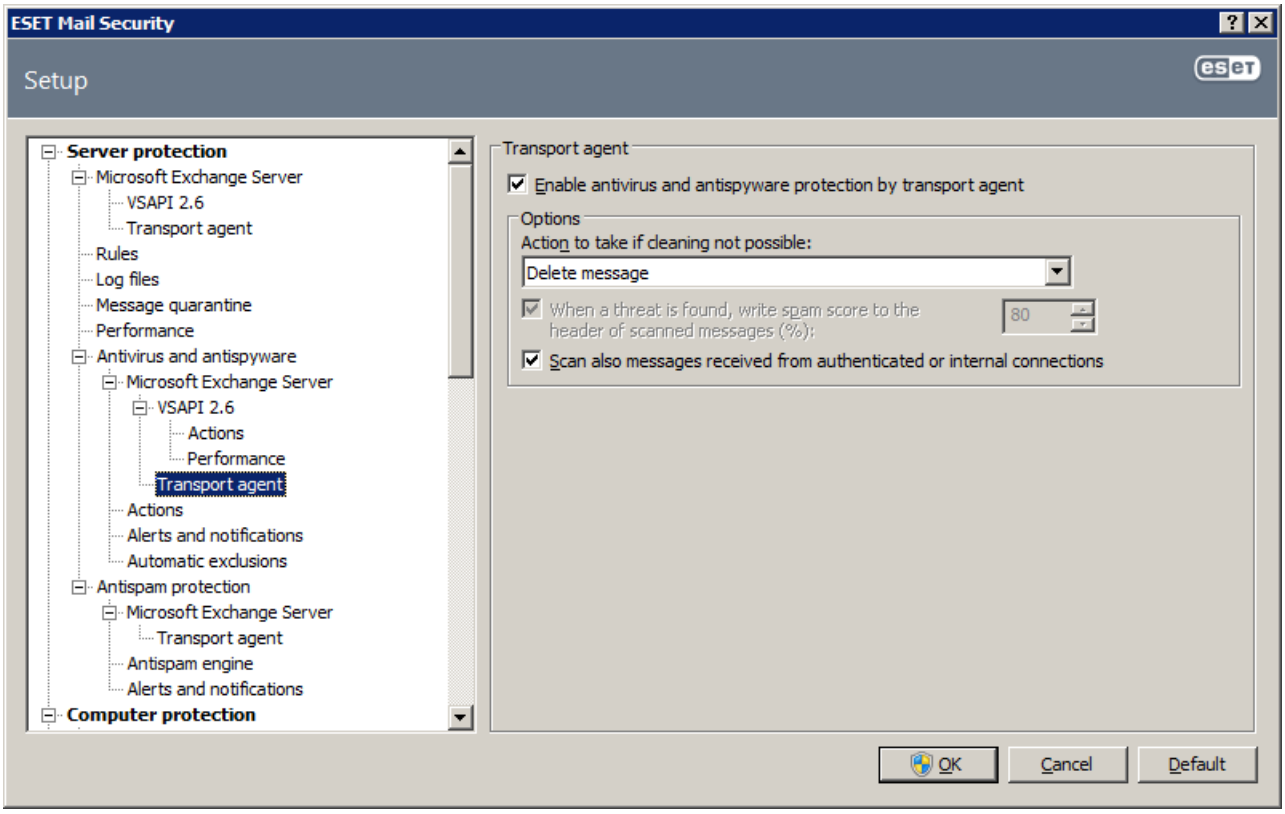
In this section you can set the number of independent scan threads used at a single time. More threads on multiprocessor machines can increase the scan rate. For the best program performance we advise using an equal number of ThreatSense scan engines and scan threads.

TIP: To determine the **Number of scan threads** the Microsoft Exchange Server provider recommends, use the following formula: [number of physical processors] x 2 + 1.

NOTE: Performance is not improved significantly if there are more ThreatSense scanning engines than scanning threads.

3.2.1.1.5 Transport Agent

In this section you can enable or disable antivirus and antispyware protection by the transport agent. For Microsoft Exchange Server 2007 and higher it is only possible to install a transport agent if the server is in one of the two roles: *Edge Transport* or *Hub Transport*.



If there is a message that cannot be cleaned, it will be processed according to the settings in Transport agent section. The message can be deleted, sent to the quarantine mailbox or retained.

If you uncheck the **Enable antivirus and antispyware protection by transport agent** option, the ESET Mail Security plug-in for Exchange server will not get unloaded from the Microsoft Exchange server process. It will only pass through the messages without scanning for viruses. The messages however, will still be scanned for spam 36 and the rules 20 will be applied.

When you **Enable antivirus and antispyware protection by transport agent** you can set **Actions to take if cleaning not possible**:

- **Retain message** – retain an infected message that could not be cleaned
- **Quarantine message** – send an infected message to the quarantine mailbox
- **Delete message** – delete an infected message

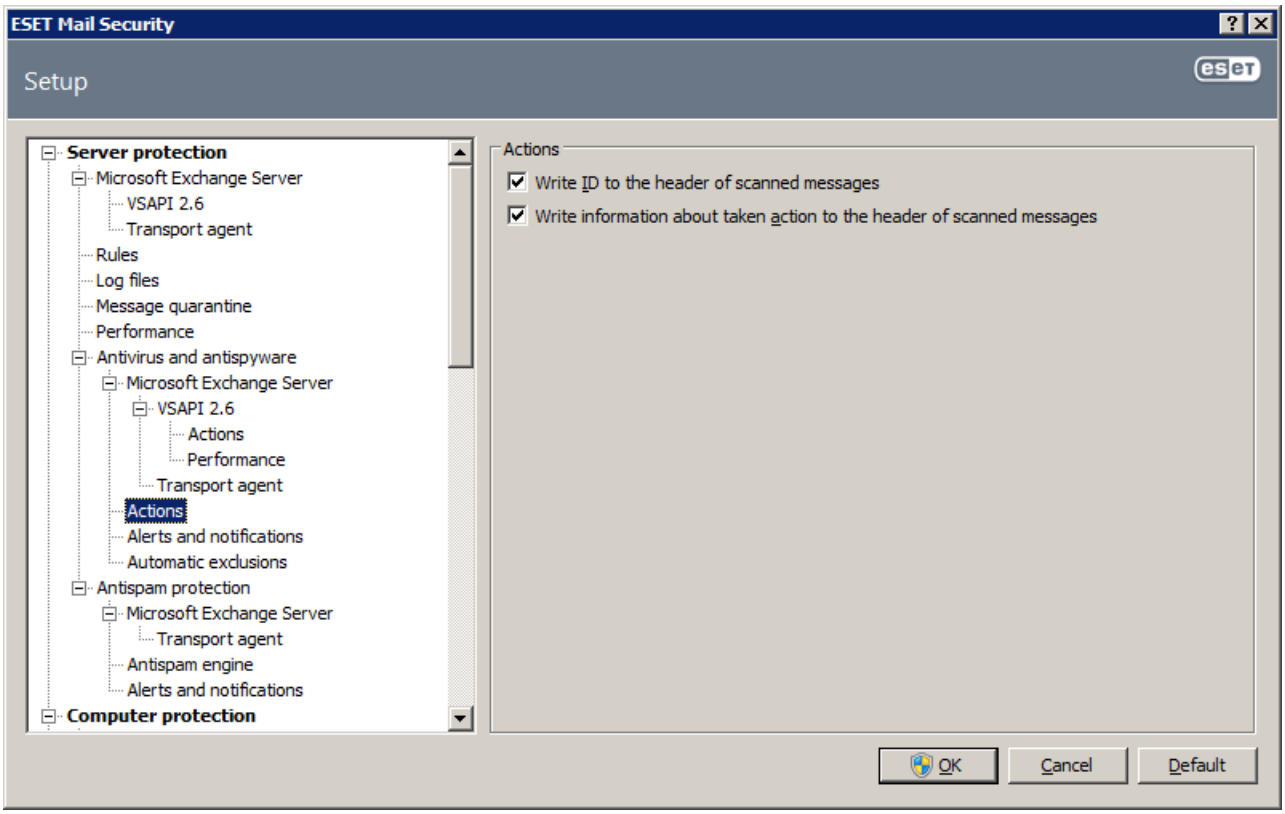
When a threat is found, write spam score to the header of scanned messages (%) – set spam score (the likelihood of the message being spam) to a specified value, expressed as a percentage

This means that if a threat is found, a spam score (specified value in %) will be written to the scanned message. Since botnets are responsible for sending the majority of infected messages, the messages distributed this way are to be categorized as spam. In order for this feature to work effectively **Write spam confidence level (SCL) to scanned messages based on spam score** option in **Server protection** > **Microsoft Exchange Server** > Transport agent 19 must be enabled.

If option **Scan also messages received from authenticated or internal connections** is enabled, ESET Mail Security also performs scanning of the messages received from authenticated sources or local servers. Scanning of such messages is recommended as it further increases protection, but it is optional.

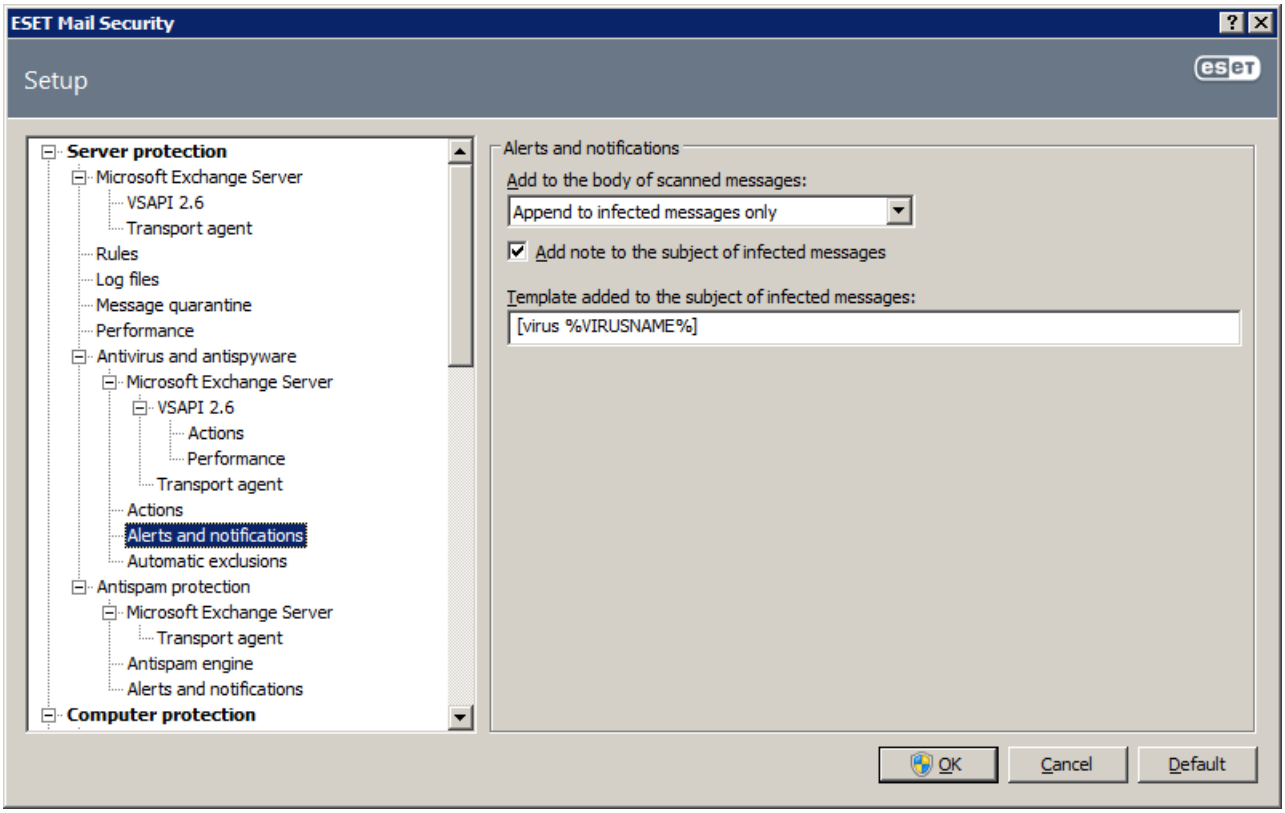
3.2.2 Actions

In this section you can choose to append a scan task ID and/or scan result information to the header of scanned messages.



3.2.3 Alerts and notifications

ESET Mail Security allows you to append text to the original subject or body of infected messages.



Add to the body of scanned messages: offers three options:

- **Do not append to messages**
- **Append to infected messages only**
- **Append to all scanned messages** (this does not apply to internal messages)

By enabling **Add to the subject of infected messages**, ESET Mail Security will append a notification tag to the email subject with the value defined in the **Template added to the subject of infected messages** text field (by default [*virus %VIRUSNAME%*]). The above-mentioned modifications can automate infected-email filtering by filtering email with a specific subject (if supported in your email client) to a separate folder.

NOTE: You can also use system variables when adding a template to the message subject.

3.2.4 Automatic exclusions

The developers of server applications and operating systems recommend excluding sets of critical working files and folders from antivirus scans for most of their products. Antivirus scans may have a negative influence on a server's performance, lead to conflicts and even prevent some applications from running on the server. Exclusions help minimize the risk of potential conflicts and increase the overall performance of the server when running antivirus software.

ESET Mail Security identifies critical server applications and server operating system files and automatically adds them to the list of Exclusions. Once added to the list, the server process/application can be enabled (by default) by checking the appropriate box or disabled by unchecking it, with the following result:

1) If an application/operating system exclusion remains enabled, any of its critical files and folders will be added to the list of files excluded from scanning (**Advanced setup** > **Computer protection** > **Antivirus and antispyware** > **Exclusions**). Every time the server is restarted, the system performs an automatic check of exclusions and restores any exclusions that may have been deleted from the list. This is the recommended setting, if you wish to make sure the recommended Automatic exclusions are always applied.

2) If the user disables an application/operating system exclusion, its critical files and folders remain on the list of files excluded from scanning (**Advanced setup** > **Computer protection** > **Antivirus and antispyware** > **Exclusions**). However, they will not be automatically checked and renewed on the **Exclusions** list every time the server is restarted (see point 1 above). We recommend this setting for advanced users, who wish to remove or modify some of the standard exclusions. If you wish to have removed the exclusions from the list without restarting the server, you will need to remove them manually from the list (**Advanced setup** > **Computer protection** > **Antivirus and antispyware** > **Exclusions)**.

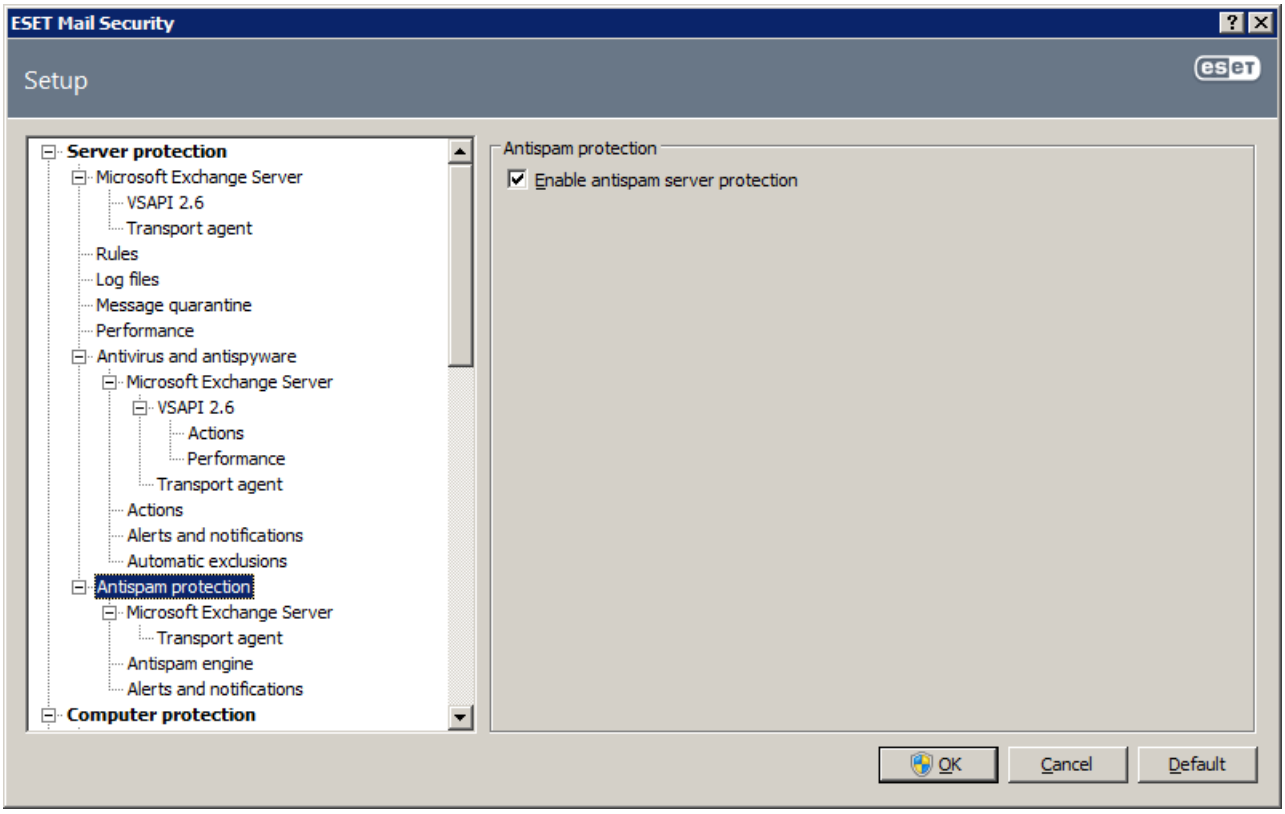
Any user-defined exclusions entered manually under **Advanced setup** > **Computer protection** > **Antivirus and antispyware** > **Exclusions** will not be affected by the settings described above.

The Automatic exclusions of server applications/operating systems are selected based on Microsoft's recommendations. For details, please see the following links:

http://support.microsoft.com/kb/822158
http://support.microsoft.com/kb/245822
http://support.microsoft.com/kb/823166
http://technet.microsoft.com/en-us/library/bb332342%28EXCHG.80%29.aspx
http://technet.microsoft.com/en-us/library/bb332342.aspx

3.3 Antispam protection

In the **Antispam protection** section, you can enable or disable spam protection for the installed mail server, configure antispam engine parameters and set other levels of protection.



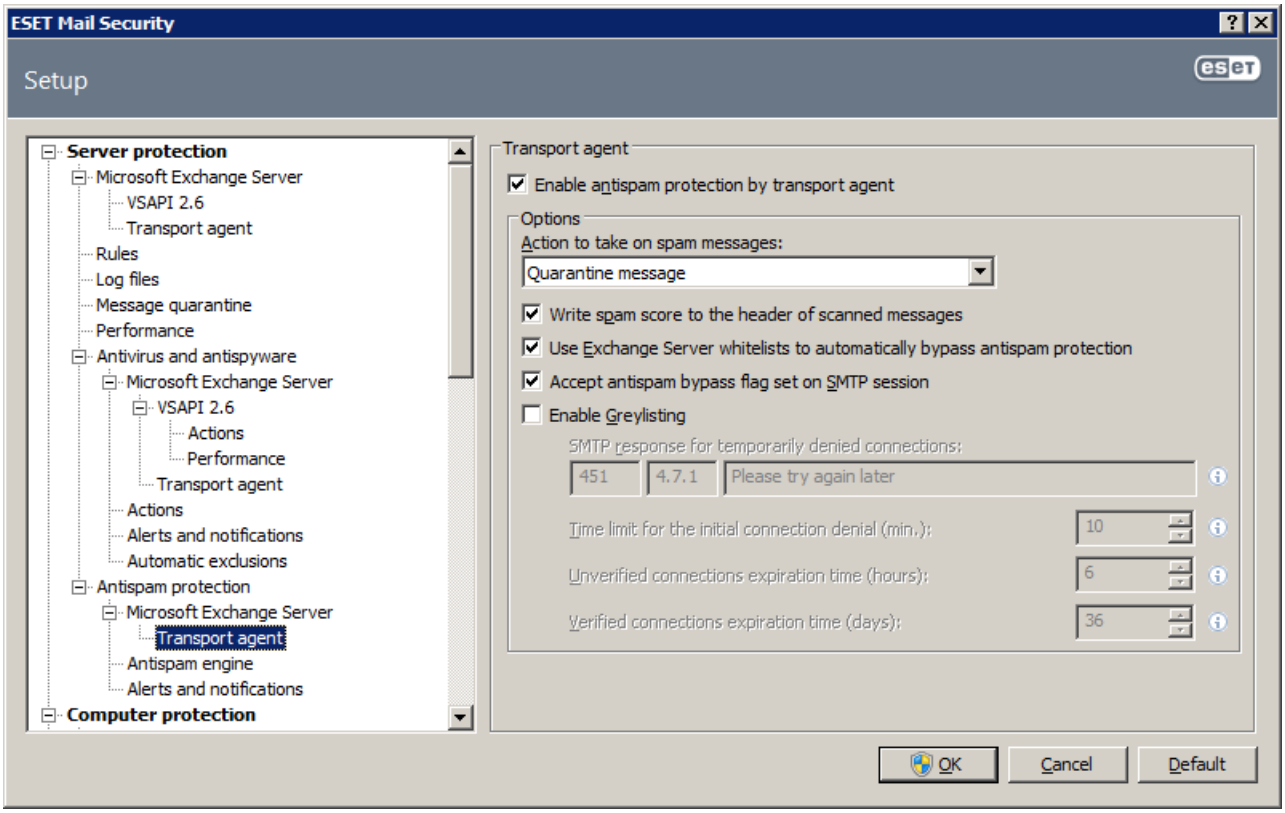
NOTE: It is necessary that the Antispam database is being updated regularly in order for the Antispam module to provide the best possible protection. To allow for correct regular updates of Antispam database, you will need to make sure that ESET Mail Security has access to particular IP addresses on particular ports. For further information on what IP's and ports to enable on your third-party firewall, read this KB article.

NOTE: Also, mirrors 85 cannot be used for Antispam database updates. For proper functioning of Antispam database updates, ESET Mail Security needs to have access to IP addresses listed in the above mentioned KB article. Without access to these IP's, Antispam module will not be able to provide most accurate results, thus the best possible protection.

3.3.1 Microsoft Exchange Server

3.3.1.1 Transport Agent

In this section you can set up options for spam protection using the transport agent.



NOTE: The transport agent is not available in Microsoft Exchange Server 5.5.

When you **Enable antispam protection by transport agent** you choose one of the following options as an **Action to take on spam messages**:

- **Retain the message** - keep the message even if it is marked as spam
- **Quarantine message** - send a message marked as spam to the quarantine mailbox
- **Delete message** – delete a message marked as spam

If you want to include information about message's spam score in its header, enable the **Write spam score to the header of scanned messages** option.

Function **Use Exchange Server whitelists to automatically bypass antispam protection** lets ESET Mail Security use specific Exchange "whitelists". When enabled, the following is taken into consideration:

- Sending sever IP address is on the Allow IP list of Exchange server
- Message recipient has Antispam Bypass flag set on his/hers mailbox
- Message recipient has sender's address on Safe Senders List (make sure you have configured Safe Senders List Synchronization within your Exchange server environment including Safelist Aggregation)

If any of the above applies to an incoming message, the antispam check will be omitted for this message, thus the message will not be evaluated for SPAM and will be delivered to the recipient's mailbox.

The **Accept antispam bypass flag set on SMTP session** is useful when you have authenticated SMTP sessions between Exchange servers with antispam bypass setting. For example, when you have an Edge server and a Hub server, there is no need for antispam scanning of the traffic between these two servers. The **Accept antispam bypass flag set on SMTP session** is enabled by default and it applies when there is antispam bypass flag configured for the SMTP session on the Exchange server. If you disable **Accept antispam bypass flag set on SMTP session** by clearing the checkbox, ESET Mail Security will be scanning the SMTP session for spam disregarding Exchange sever antispam bypass setting.

The **Enable Greylisting** function activates a feature that protects users from spam using the following technique: The transport agent will send a "temporarily reject" SMTP return value (default is 451/4.7.1) for any received email

that is not from a recognized sender. A legitimate server will try to resend the message after a delay. Spam servers will typically not attempt to resend the message, as they usually go through thousands of email addresses and do not waste time resending. Greylisting is an additional layer of antispam protection and does not have any effect on the spam evaluation capabilities of the antispam module.

When evaluating the message source the method takes into account the configurations of the **Approved IP addresses** list, the **Ignored IP addresses** list, the **Safe Senders** and the **Allow IP** lists on the Exchange server and the AntispamBypass settings for the recipient mailbox. Emails from these IP addresses/senders lists or emails delivered to a mailbox that has the AntispamBypass option enabled will be bypassed by the greylisting detection method.

The **SMTP response for temporarily denied connections** field defines the SMTP temporary denial response sent to the SMTP server if a message is refused.

Example of SMTP response message:

Primary response code	Complementary status code	Description
451	4.7.1	Requested action aborted: local error in processing

Warning: Incorrect syntax in SMTP response codes may lead to malfunctioning of greylisting protection. As a result, spam messages may be delivered to clients or messages may not be delivered at all.

Time limit for the initial connection denial (min.) - when a message is delivered for the first time and temporarily refused, this parameter defines the time period during which the message will always be refused (measured from the first refusal). After the defined time period has elapsed, the message will be successfully received. The minimum value you can enter is 1 minute.

Unverified connections expiration time (hours) – this parameter defines the minimum time interval for which the triplet data will be stored. A valid server must resend a desired message before this period expires. This value must be greater than the value of **Time limit for the initial connection denial**.

Verified connections expiration time (days) – the minimum number of days for which the triplet information is stored, during which emails from a particular sender will be received without any delay. This value must be greater than the value of **Unverified connections expiration time**.

NOTE: You can also use system variables when defining the SMTP reject response.

3.3.1.2 POP3 Connector and antispam

Microsoft Windows Small Business Server (SBS) versions includes POP3 Connector that enables the server to fetch email messages from external POP3 servers. Implementation of this "standard" POP3 Connector differs from one SBS version to another.

ESET Mail Security does support Microsoft SBS POP3 Connector on SBS 2008 and messages downloaded via this POP3 Connector are scanned for the presence of spam. This works because messages are being transported into the Microsoft Exchange via SMTP. However, Microsoft SBS POP3 Connector on SBS 2003 is not supported by ESET Mail Security, thus massages are not scanned for spam. This is because messages actually bypass SMTP queue.

There also exist a number of third party POP3 Connectors. Whether messages fetched via certain POP3 Connector are scanned for spam or not depend on the actual method this POP Connector is using to fetch messages. For example, GFI POP2Exchange transports messages via Pickup Directory, thus messages are not scanned for spam. Similar issues may appear with products which transport messages via authenticated session (such as IGetMail), alternatively when Microsoft Exchange marks these as internal messages for which antispam is bypassed by default. This setting can be changed in configuration file. Export configuration into xml, change `AgentASScanSecureZone` setting's value to `"1"` and import the configuration back (for details on how to import and export configuration file see chapter Import and export settings 122). You can also try disabling **Accept antispam bypass flag set on SMTP session** in F5 advanced setup tree under **Server protection** > **Antispam protection** > **Microsoft Exchange Server** > **Transport agent**. By doing this, ESET Mail Security will be scanning the SMTP session for spam disregarding Exchange sever antispam bypass setting.

3.3.2 Antispam engine

In here, you can configure **Antispam engine** parameters. You can do so by clicking on **Setup...** button. A window will open where you can configure these Antispam engine parameters.

Message categorization

The ESET Mail Security Antispam engine assigns a spam score from 0 to 100 to every scanned message. By changing the limits of spam scores in this section, you can influence:

1) whether a message will be classified as SPAM or not-SPAM. All messages that have a spam score equal to or higher than the **Spam score to treat a message as spam:** value are considered SPAM. As a consequence, actions set in the Transport agent 36 will be applied to these messages.

2) if a message will be recorded in the antispam log 92 (**Tools** > **Log files** > **Antispam**). All messages that have a spam score value equal to or higher than the **Spam score threshold to treat a message as probable spam or probable clean:** value are recorded by the log.

3) what section of antispam statistics will the message in question be counted in (**Protection status > Statistics > Mail server antispam protection**):

Messages evaluated as SPAM – the message's spam score is equal to or higher than the value set for **Spam score to treat message as spam:**

Messages evaluated as probably SPAM: - the message's spam score is equal to or higher than the value set for **Spam score threshold to treat a message as probable spam or probable clean:**

Messages evaluated as probably NOT SPAM - the message's spam score is lower that the value set for **Spam score threshold to treat a message as probable spam or probable clean:**

Messages evaluated as NOT SPAM – the message's spam score is equal or lower than the value set for **Spam score to treat message as not spam:**

3.3.2.1 Antispam engine parameter setup

3.3.2.1.1 Analysis

In this section, you can configure how messages are analysed for SPAM and subsequently processed.

Scan message attachments - This option lets you choose whether the antispam engine will scan and consider attachments when computing the spam score.

Use both MIME sections - The antispam engine will analyze both text/plain and text/html MIME sections in a message. If additional performance is desired, it is possible to only analyze one section. If this option is unchecked (disabled), then only one section will be analyzed.

Memory size for score calculation (in bytes): - This option instructs the antispam engine not to read more than a configurable number of bytes from the message buffer when processing rules.

Memory size for sample calculation (in bytes): - This option instructs the antispam engine not to read more than the defined bytes when computing the message fingerprint. This is useful for getting consistent fingerprints.

Use LegitRepute cache memory - Enables usage of a LegitRepute cache to reduce false positives especially for newsletters.

Convert to UNICODE - Improves accuracy and throughput for email message bodies in Unicode especially double-byte languages by converting the message into single-bytes.

Use domain cache memory - Enables usage of a domain reputation cache. If enabled, domains are extracted from messages and compared against a domain reputation cache.

3.3.2.1.1.1 Samples

Use cache memory - Enables usage of a fingerprint cache (Enabled by default).

Turn on MSF - Allows for use of an alternate fingerprinting algorithm known as MSF. When enabled, you will be able to set following limits and thresholds:

- **Number of messages designating a bulk message:** - This option specifies how many similar messages are required in order to consider a message bulk.
- **Frequency of clearing cache memory:** - This option specifies an internal variable which determines how frequently the in-memory MSF cache is pruned.
- **Two samples match sensitivity:** - This option specifies the match percentage threshold for two fingerprints. If the match percentage is higher than this threshold then messages are considered to be the same.
- **Number of samples stored in memory:** - This option specifies the number of MSF fingerprints to keep in memory. The higher the number, the more memory is used but also the higher the accuracy.

3.3.2.1.1.2 SpamCompiler

Turn on SpamCompiler - Speeds up rules processing but requires a little bit more memory.

Preffered version: - Specifies what SpamCompiler version to use. When set to **Automatic**, the antispam engine will choose the best engine to use.

Use cache memory - If this option is enabled, SpamCompiler will store the compiled data on disk instead of memory in order to reduce memory usage.

List of cache memory files: - This option specifies which rules files are compiled on disk instead of memory.

Set rule files indexes which will be stored in cache memory on disk. To manage rule file indexes you can:

- **Add...**
- **Edit..**
- **Remove**

NOTE: Only numbers are acceptable characters.

3.3.2.1.2 Training

Use training for message fingerprint score - Enables fingerprint score offset training.

Use training words - This option controls whether Bayesian Word Token analysis is used. Accuracy can be greatly improved but more memory is used and it is slightly slower.

- **Number of words in cache memory:** - This option specifies the number of word tokens to cache at any time. The higher the number, the more memory is used but also the higher the accuracy. To enter the number, enable option **Use training words** first.

Use training database only for reading: - This option controls whether the word, rules, and fingerprint training databases can be modified or are read-only after the initial load. A read-only training database is faster.

- **Automatic training sensitivity:** - Sets a threshold for auto-training. If a message is scored at or above the high threshold, that message is considered a definite spam and is then used to train all the enabled Bayesian modules (rules and/or word) but not sender or fingerprint. If a message is scored at or below the low threshold, that message is considered a definite ham and is then used to train all the enabled Bayesian modules (rules and/or word) but not sender or fingerprint. To enter the high and low threshold number, enable option **Use training database only for reading:** first.

Minimum amount of training data: - Initially, only the rule weights are used to compute the spam score. Once a minimum set of training data is achieved, rule/word training data replaces the rule weights. The default minimum is 100 which means that it must be trained on at least 100 equivalent known ham messages and 100 equivalent spam messages for a total of 200 messages before the training data replaces the rule weights. If the number is too low then the accuracy could be poor due to insufficient data. If the number is too high, then the training data will not be fully taken advantage of. A value of 0 will cause rule weights to always be ignored.

Use only training data - Controls whether to give full weight to training data. If this option is enabled then scoring will be based solely on training data. If this option is disabled (unchecked) then both rules and training data will be used.

Number of scanned messages before writing them to disk: - While training, the antispam engine will process a configurable amount of messages before writing the training database to disk. This option determines how many messages to process before writing to disk. For maximum performance, this number should be as large as possible. In an unusual case when a program is unexpectedly terminated before buffer has been written to disk, the training performed since the last disk write will be lost. The buffer is written to disk on normal termination.

Use country data for training - Controls whether country routing information should be considered when training and scoring messages.

3.3.2.1.3 Rules

Use rules - This option controls whether slower heuristic rules are used. Accuracy can be greatly improved but more memory is used and it is much slower.

- **Use rule set extension** - Enables the extended rule set.
- **Use second rule set extension** - Enables the second extension to rule set.

Custom Rule weight: - This option allows overriding weights associated with individual rules.

List of downloaded rule files: - This option specifies which rule files are downloaded.

Category weight: - Allows the end user to adjust the weights of categories used in sc18 and in files used in custom rules list. Category: Name of category, currently limited to SPAM, PHISH, BOUNCE, ADULT, FRAUD, BLANK, FORWARD and REPLY. This field is case insensitive. Score: Any integer or BLOCK or APPROVE. The weight of rules matching the corresponding category will be multiplied by the scaling factor to produce a new effective weight.

Custom rules list: - Allows user to specify a custom list of rules (i.e. spam, ham, or phishing words/phrases). Custom rules files contain phrases in the following format on separate lines: phrase, type, confidence, caseSensitivity phrase can be any text except commas. Any commas in the phrase should be deleted. type can be either SPAM, PHISH, BOUNCE, ADULT, or FRAUD. If anything other than those are specified, the TYPE is automatically assumed to be SPAM. Confidence can be from 1 to 100. If type is SPAM, then 100 indicates a higher confidence of spamminess. If type is PHISH, then 100 indicates a higher confidence of phishiness. If type is BOUNCE, then 100 indicates a higher confidence that phrase is related to bounces. A higher confidence is more likely to impact the final score. A value of 100 is a special case. If type is SPAM, then 100 will score the message as 100. If type is PHISH, then 100 will score the message as 100. If type is BOUNCE, then 100 will score the message as 100. As always, any whitelist overrides any blacklist. caseSensitivity value of 1 means that the phrase will be case sensitive; 0 means that the phrase will be case insensitive. Examples:

spamming is fun, SPAM, 100,0
phishing is Phun, PHISH, 90,1
return to sender, BOUNCE, 80,0

The first line means that all variations of "spamming is fun" are considered as SPAM with a confidence of 100. The phrase is case insensitive. The second line means that all variations of "phishing is phun" are considered as PHISH with a confidence 90. The phrase is case sensitive. The third line means that all variations of " return to sender " are considered as BOUNCE with a confidence 80. The phrase is case insensitive.

Clear older rules after their update - The antispam engine, by default, will clean up older rule files from the configuration directory when a new file is retrieved from the SpamCatcher network. However, some users of the antispam engine will want to archive older rule files. This can be done by disabling this cleanup feature.

Show notification after successful update of rules

3.3.2.1.3.1 Rule weight

Set rule file indexes and their weight. To add a rule weight, press **Add...** button. To modify existing, press **Edit...** button. To delete, press **Remove** button.

Specify **Index:** and **Weight:** values.

3.3.2.1.3.2 List of downloaded rule files

Set rule file indexes which should be downloaded to disk. Use **Add**, **Edit** and **Remove** buttons to manage rule file indexes.

3.3.2.1.3.3 Category weight

Set rule categories and their weight. Use **Add...**, **Edit...** and **Remove** button to manage categories and their weight.

To add a category weight select a **Category:** from list. Available are:

- **SPAM**
- **Phishing**
- **Non-delivery report**
- **Mature content messages**
- **Fraudulent messages**
- **Empty messages**
- **Forwarding messages**
- **Replying messages**

Then select an action:

- **Allow**
- **Block**
- **Weight:**

3.3.2.1.3.4 Custom rules list

You can use custom rules files that contain phrases. These files are basically .txt files, for details and phrase format see Rules 40 topic (section **Custom rules list**).

To use files containing custom rules which will be used for message analysis, you need to place them in following location:

in case you run Windows Server 2008 and newer, the path is:
C:\ProgramData\ESET\ESET Mail Security\ServerAntispam

in case of Windows Server 2003 and older, the path is:
C:\Documents and Settings\All Users\Application Data\ESET\ESET Mail Security\ServerAntispam

To get the files loaded press **...** (browse) button, navigate to location mentioned above and select text file (*.txt). Use **Add**, **Edit** and **Remove** buttons to manage custom rules list.

NOTE: The .txt file containing custom rules must be placed in the *ServerAntispam* folder, otherwise this file will not be loaded.

3.3.2.1.4 Filtering

In this section, you can configure allowed, blocked and ignored lists by specifying criteria such as IP address or range, domain name, email address, etc. To add, modify or remove criteria, simply navigate to the list you want to manage and click on the appropriate button to do so.

3.3.2.1.4.1 Allowed senders

Whitelisted senders and domains can contain an email address or a domain. Addresses are entered in the format "mailbox@domain" and domains simply in the format "domain".

NOTE: Leading and trailing white space is ignored, regular expressions are not supported and asterisk "*" is ignored as well.

3.3.2.1.4.2 Blocked senders

Blacklisted senders and domains can contain an email address or a domain. Addresses are entered in the format "mailbox@domain" and domains simply in the format "domain".

NOTE: Leading and trailing white space is ignored, regular expressions are not supported and asterisk "*" is ignored as well.

3.3.2.1.4.3 Allowed IP addresses

This option allows you to specify IP's which should be approved. Ranges can be specified in three ways:

a) starting IP - ending IP
b) IP address and network mask
c) IP address

If the first non-ignored IP in Received: headers match any in this list then message is scored a 0 and no other checks are made.

3.3.2.1.4.4 Ignored IP addresses

This option allows you to specify IP's which should be ignored when doing RBL checks. The following are always implicitly ignored:

10.0.0.0/8, 127.0.0.0/8, 192.168.0.0/16, 172.16.0.0

Ranges can be specified in three ways:

a) starting IP - ending IP
b) IP address and network mask
c) IP address

3.3.2.1.4.5 Blocked IP addresses

This option allows you to specify IP's which should be blocked. Ranges can be specified in three ways:

a) starting IP - ending IP
b) IP address and network mask
c) IP address

If any IP addresses in Received: headers match any in this list then message is scored a 100 and no other checks are made.

3.3.2.1.4.6 Allowed domains

This option allows you to specify body domains and IP's which should should always be approved.

3.3.2.1.4.7 Ignored domains

This option allows you to specify body domains which should always be excluded from the DNSBL checks and ignored.

3.3.2.1.4.8 Blocked domains

This option allows you to specify body domains and IP's which should should always be blocked.

3.3.2.1.4.9 Spoofed senders

Allows blocking spammers who spoof your domain name and other domain names. For example, spammers often use the recipient's domain name as the From: domain name. This list allows you to specify which mail servers are allowed to use which domain names in the From: address. The offset will be applied when mail from the domain does not come from the specified IP range.

3.3.2.1.5 Verification

Verification is an additional feature of Antispam protection. It allows for messages being verified by the means of external servers according to defined criteria. Choose a list from the setup tree to configure its criteria. The lists are following:

- **RBL** (Realtime Blackhole List)
- **LBL** (Last Blackhole List)
- **DNSBL** (DNS Blocklist)

3.3.2.1.5.1 RBL (Realtime Blackhole List)

RBL servers: - Specifies a list of Realtime Blackhole List (RBL) servers to query when analyzing messages. Please refer to the RBL section in this document for further information.

RBL verification sensitivity: - Since RBL checks can introduce latency and a decrease in performance, this option allows running RBLs check conditionally based on the score prior to RBL checks. If score is greater than the "high" value then only those RBL servers which can bring score below "high" value are queried. If score is less than the "low" value then only those RBL servers which can bring score above "low" value are queried. If score is between "low" and "high" then all RBL servers are queried.

RBL request execution limit (in seconds): - This option allows setting a maximum timeout for finishing all RBL queries. RBL responses are only used from those RBL servers which responded in time. If value is "O" then no timeout is enforced.

Maximum number of verified addresses against RBL: - This option allows limiting how many IP addresses are queried against the RBL server. Note that the total number of RBL queries will be the number of IP addresses in the Received: headers (up to a maximum of RBL maxcheck IP addresses) multiplied by the number of RBL servers specified in RBL list. If the value is "O" then unlimited number of received headers are checked. Note that IP's which match against the ignored IP list option do not count towards the RBL IP addresses limit.

To manage the list, use **Add...**, **Edit...** or **Remove** buttons.

The list consists of three columns:

Address
Response
Score

3.3.2.1.5.2 LBL (Last Blackhole List)

LBL servers: - The Last Connecting IP is queried against the LBL server. You can specify a different DNS lookup for the last connecting incoming IP. For the last connecting incoming IP, the LBL list is queried instead of RBL list. Otherwise, the RBL list options such as RBL threshold are also applied to the LBL list.

IP addresses not verified against LBL: - If the Last Connecting IP matches with an IP on the list, then that IP is queried against the RBL server(s) instead of the LBL server(s).

To manage the list, use **Add...**, **Edit...** or **Remove** buttons.

The list consists of three columns:

Address
Response
Score

Here, you can specify IP addresses which will not be verified against LBL. To manage the list, use **Add...**, **Edit...** or **Remove** buttons.

3.3.2.1.5.3 DNSBL (DNS Block List)

DNSBL servers: - Specifies a list of DNS Blocklist (DNSBL) servers to query with domains and IP's extracted from the message body.

DNSBL verification sensitivity: - If score is greater than the "high" value then only those DNSBL servers which can bring score below "high" value are queried. If score is less than the "low" value then only those DNSBL servers which can bring score above "low" value are queried. If score is between "low" and "high" then all DNSBL servers are queried.

DNSBL request execution limit (in seconds): - Allows setting a maximum timeout for finishing all DNSBL queries.

Maximum number of verified domains against DNSBL: - Allows limiting how many domains and IP's are queried against the DNS Blocklist server.

To manage the list, use **Add...**, **Edit...** or **Remove** buttons.

The list consists of three columns:

Address
Response
Score

3.3.2.1.6 DNS

Use cache memory - Enable internal caching of DNS requests.

Number of DNS requests stored in memory: - Limits the number of entries in internal DNS cache.

Save cache memory to disk - If enabled, DNS cache will store entries on disk on shutdown and read from disk on initialization.

DNS server address: - DNS servers can now be explicitly specified to override the default.

Direct DNS access: - When set to yes and if DNS server is not specified, then the antispam engine will make LiveFeed requests directly to the LiveFeed servers. This option is ignored if DNS server is specified as it has precedence. This option should be set to **Yes** when direct queries are more efficient than the default DNS servers.

DNS request lifetime (in seconds): - This option allows setting a minimum TTL for entries in the antispam engine's internal DNS cache. The option is specified in seconds. For those DNS responses whose TTL value is less than specified minimum TTL, the antispam engine's internal cache will use specified TTL instead of the TTL value of the DNS response.

3.3.2.1.7 Score

Turn on score history - Enables tracking of historical scores for repeat senders.

Stop analysis when SPAM score threshold has been reached - This option allows you to tell the antispam engine to stop analyzing the message once a score has been reached. This can reduce the number of rules and other checks that are performed, thus improving throughput.

Use accelerated analysis before threshold score for a clean message has been reached - This option allows you to tell the antispam engine to skip slow rule checks if the message is likely to be ham.

Message categorization

- **Score value from which a message is regarded as SPAM:** - Antispam engine assigns scanned message a score from 0 to 100. Setting the score value borders affects what messages are considered as SPAM and what messages aren't. If you set incorrect values, it may decrease quality of the antispam engine's detection results.
- **Score value which sets a border when a message is regarded as probable SPAM or probably clean:** - Antispam engine assigns scanned message a score from 0 to 100. Setting the score value borders affects what messages are considered as SPAM and what messages aren't. If you set incorrect values, it may decrease quality of the antispam engine's detection results.
- **Score value up to which a message is regarded as certainly clean:** - Antispam engine assigns scanned message a score from 0 to 100. Setting the score value borders affects what messages are considered as SPAM and what messages aren't. If you set incorrect values, it may decrease quality of the antispam engine's detection results.

3.3.2.1.8 Spambait

Spam addresses: - If the RCPT TO: address from SMTP envelope matches an email address in this list, then the statistics file will record tokens in email message as being sent to a spambait address. Addresses must match exactly ignoring case, wildcard entries are not supported.

Addresses regarded as nonexistent: - If the RCPT TO: address from SMTP envelope matches an email address in this list, then the statistics file will record tokens in email message as being sent to a nonexistent address. Addresses must match exactly ignoring case, wildcard entries are not supported.

3.3.2.1.8.1 Spambait addresses

You can set email addresses which will only receive SPAM. To add an email address, type it in a standard format and press **Add** button. To modify existing email address, use **Edit** button. To delete, press **Remove** button.

3.3.2.1.8.2 Addresses regarded as nonexistent

You can set email addresses which will appear as nonexistent to the outside. To add an email address, type it in a standard format and press **Add** button. To modify existing email address, use **Edit** button. To delete, press **Remove** button.

3.3.2.1.9 Communication

Single SpamLabs request duration (in seconds): - Limit how long single request to the Antispam protection SpamLabs can take. The value is specified in units of integral seconds. The value of "0" disables this feature and no limit will be placed.

Use v.4x protocol: - Communicate with the Antispam protection SpamLabs to determine scoring via old slower v4.x protocol. When you set this option to **Automatically**, it allows Antispam engine to automatically use the netcheck feature as a fallback to LiveFeed queries.

- **Range of v4.x protocol usage:** - Since networks can introduce latency and a decrease in performance, this option allows running network checks conditionally based on the score. Network is only queried if score is at or between the "low" and "high" range specified via this option.

LiveFeed server address: - Specifies which server to query for LiveFeed requests.

LiveFeed request lifetime (in seconds): - This option allows setting a minimum TTL for entries in the antispam

engine's internal LiveFeed cache. The option is specified in seconds. For those LiveFeed responses whose TTL value is less than specified minimum TTL, the antispam engine's internal cache will use specified TTL instead of the TTL value of the LiveFeed response.

Proxy server authentication type: - Specifies what type of a HTTP proxy authentication should be used.

3.3.2.1.10 Performance

Maximum size of the used thread stack: - Sets the maximum thread stack size to use. If the thread stack size is set to 64KB, then this variable should be set to 100 or less. If the thread stack size is set to greater than 1MB, then this variable should be set to 10000 or less. If this variable is set below 200, accuracy can be reduced by a couple of percentages.

Required throughput (in messages per second): - This option allows you to specify the desired throughput in messages per second. The antispam engine will attempt to reach that level by optimizing the rules that are run. It is possible that accuracy may be reduced. A value of 0 disables the option.

Join incremental files into one - The antispam engine, by default, will merge multiple incr files and a full file into a single updated full file. This is done to reduce file clutter in the configuration directory.

Download only incremental files - The antispam engine, by default, will attempt to download the most size efficient combination of full and incr file. The antispam engine can be forced to only download incr file by setting this option to yes.

Maximum size of incremental files: - In order to reduce cpu usage while rule files are updated, the on-disk cache files (sc*.tmp) are no longer regenerated on every single rule update. Instead they are regenerated when there is a newer sc*.bin.full file or when the sum of the sc*.bin.incr grows beyond the number of bytes specified in maximum size of incremental files.

Temporary files location: - This parameter controls where the antispam engine will create temporary files.

3.3.2.1.11 Regional settings

List of home languages: - This option permits you to set languages which are preferred in your email messages. The country codes are two character ISO-639 language codes.

List of home countries: - This option allows specifying a list of countries which are considered "home" countries. Messages routed through a country which is not on this list will be scored more aggressively. If this option is empty then no penalty will occur.

List of blocked countries: - Allows blocking by country. If an IP address in a received header matches a listed country the email will be considered as SPAM. The country codes aren't applied to sender addresses. Note that it is possible for a message to have traveled through various countries before reaching the final destination. Also, this option is only 98% accurate so blocking countries can result in false positives.

List of blocked charsets: - Allows blocking by character-set. Default SPAM score value is set to 100, but you can adjust it for each blocked char-set separately. Note that language to char-set mapping is not 100% accurate so blocking char-sets can result in false positives.

3.3.2.1.11.1 List of home languages

Set languages which you consider as home languages and in which you prefer to receive messages. To add a home language, select it from the **Language codes:** column and press **Add** button. This will move the language to the **"Home" languages** column. To remove the language from **"Home" languages** column, select its code and press **Remove** button.

Block non-home languages: - This option controls whether or not languages, which are not listed in the "Home" column, will be blocked. There are three options:

- **Yes**
- **No**
- **Automatically**

List of language codes (based on ISO 639):

Afrikaans	af
Amharic	am

Arabic	ar
Byelorussian	be
Bulgarian	bg
Catalan	ca
Czech	cs
Welsh	cy
Danish	da
German	de
Greek	el
English	en
Esperanto	eo
Spanish	es
Estonian	et
Basque	eu
Persian	fa
Finnish	fi
French	fr
Frisian	fy
Irish	ga
Gaelic	gd
Hebrew	he
Hindi	hi
Croatian	hr
Hungarian	hu
Armenian	hy
Indonesian	id
Icelandic	is
Italian	it
Japanese	ja
Georgian	ka
Korean	ko
Latin	la
Lithuanian	lt
Latvian	lv
Marathi	mr
Malay	ms
Nepali	ne
Dutch	nl
Norwegian	no
Polish	pl
Portuguese	pt
Quechua	qu
Rhaeto-Romance	rm
Romanian	ro
Russian	ru
Sanskrit	sa
Scots	sco
Slovak	sk
Slovenian	sl
Albanian	sq
Serbian	sr
Swedish	sv
Swahili	sw
Tamil	ta
Thai	th
Tagalog	tl
Turkish	tr
Ukrainian	uk
Vietnamese	vi
Yiddish	yi
Chinese	zh

3.3.2.1.11.2 List of home countries

Set countries which you consider as home countries and from which you prefer to receive messages. To add a home country, select it from the **Country code:** column and press **Add** button. This will move the country to the **"Home" countries** column. To remove the country from **"Home" countries** column, select the country code and press **Remove** button.

List of country codes (based on ISO 3166):

AFGHANISTAN	AF
ÅLAND ISLANDS	AX
ALBANIA	AL
ALGERIA	DZ
AMERICAN SAMOA	AS
ANDORRA	AD
ANGOLA	AO
ANGUILLA	AI
ANTARCTICA	AQ
ANTIGUA AND BARBUDA	AG
ARGENTINA	AR
ARMENIA	AM
ARUBA	AW
AUSTRALIA	AU
AUSTRIA	AT
AZERBAIJAN	AZ
BAHAMAS	BS
BAHRAIN	BH
BANGLADESH	BD
BARBADOS	BB
BELARUS	BY
BELGIUM	BE
BELIZE	BZ
BENIN	BJ
BERMUDA	BM
BHUTAN	BT
BOLIVIA	BO
BOSNIA AND HERZEGOVINA	BA
BOTSWANA	BW
BOUVET ISLAND	BV
BRAZIL	BR
BRITISH INDIAN OCEAN TERRITORY	IO
BRUNEI DARUSSALAM	BN
BULGARIA	BG
BURKINA FASO	BF
BURUNDI	BI
CAMBODIA	KH
CAMEROON	CM
CANADA	CA
CAPE VERDE	CV
CAYMAN ISLANDS	KY
CENTRAL AFRICAN REPUBLIC	CF
CHAD	TD
CHILE	CL
CHINA	CN
CHRISTMAS ISLAND	CX
COCOS (KEELING) ISLANDS	CC
COLOMBIA	CO
COMOROS	KM
CONGO	CG
CONGO, THE DEMOCRATIC REPUBLIC OF THE	CD
COOK ISLANDS	CK
COSTA RICA	CR

CÔTE D'IVOIRE	CI
CROATIA	HR
CUBA	CU
CYPRUS	CY
CZECH REPUBLIC	CZ
DENMARK	DK
DJIBOUTI	DJ
DOMINICA	DM
DOMINICAN REPUBLIC	DO
ECUADOR	EC
EGYPT	EG
EL SALVADOR	SV
EQUATORIAL GUINEA	GQ
ERITREA	ER
ESTONIA	EE
ETHIOPIA	ET
FALKLAND ISLANDS (MALVINAS)	FK
FAROE ISLANDS	FO
FIJI	FJ
FINLAND	FI
FRANCE	FR
FRENCH GUIANA	GF
FRENCH POLYNESIA	PF
FRENCH SOUTHERN TERRITORIES	TF
GABON	GA
GAMBIA	GM
GEORGIA	GE
GERMANY	DE
GHANA	GH
GIBRALTAR	GI
GREECE	GR
GREENLAND	GL
GRENADA	GD
GUADELOUPE	GP
GUAM	GU
GUATEMALA	GT
GUINEA	GN
GUINEA-BISSAU	GW
GUYANA	GY
HAITI	HT
HEARD ISLAND AND MCDONALD ISLANDS	HM
HOLY SEE (VATICAN CITY STATE)	VA
HONDURAS	HN
HONG KONG	HK
HUNGARY	HU
ICELAND	IS
INDIA	IN
INDONESIA	ID
IRAN, ISLAMIC REPUBLIC OF	IR
IRAQ	IQ
IRELAND	IE
ISRAEL	IL
ITALY	IT
JAMAICA	JM
JAPAN	JP
JORDAN	JO
KAZAKHSTAN	KZ
KENYA	KE
KIRIBATI	KI
KOREA, DEMOCRATIC PEOPLE'S REPUBLIC OF	KP
KOREA, REPUBLIC OF	KR

KUWAIT	KW
KYRGYZSTAN	KG
LAO PEOPLE'S DEMOCRATIC REPUBLIC	LA
LATVIA	LV
LEBANON	LB
LESOTHO	LS
LIBERIA	LR
LIBYAN ARAB JAMAHIRIYA	LY
LIECHTENSTEIN	LI
LITHUANIA	LT
LUXEMBOURG	LU
MACAO	MO
MACEDONIA, THE FORMER YUGOSLAV REPUBLIC OF	MK
MADAGASCAR	MG
MALAWI	MW
MALAYSIA	MY
MALDIVES	MV
MALI	ML
MALTA	MT
MARSHALL ISLANDS	MH
MARTINIQUE	MQ
MAURITANIA	MR
MAURITIUS	MU
MAYOTTE	YT
MEXICO	MX
MICRONESIA, FEDERATED STATES OF	FM
MOLDOVA, REPUBLIC OF	MD
MONACO	MC
MONGOLIA	MN
MONTSERRAT	MS
MOROCCO	MA
MOZAMBIQUE	MZ
MYANMAR	MM
NAMIBIA	NA
NAURU	NR
NEPAL	NP
NETHERLANDS	NL
NETHERLANDS ANTILLES	AN
NEW CALEDONIA	NC
NEW ZEALAND	NZ
NICARAGUA	NI
NIGER	NE
NIGERIA	NG
NIUE	NU
NORFOLK ISLAND	NF
NORTHERN MARIANA ISLANDS	MP
NORWAY	NO
OMAN	OM
PAKISTAN	PK
PALAU	PW
PALESTINIAN TERRITORY, OCCUPIED	PS
PANAMA	PA
PAPUA NEW GUINEA	PG
PARAGUAY	PY
PERU	PE
PHILIPPINES	PH
PITCAIRN	PN
POLAND	PL
PORTUGAL	PT
PUERTO RICO	PR
QATAR	QA

RÉUNION	RE
ROMANIA	RO
RUSSIAN FEDERATION	RU
RWANDA	RW
SAINT HELENA	SH
SAINT KITTS AND NEVIS	KN
SAINT LUCIA	LC
SAINT PIERRE AND MIQUELON	PM
SAINT VINCENT AND THE GRENADINES	VC
SAMOA	WS
SAN MARINO	SM
SAO TOME AND PRINCIPE	ST
SAUDI ARABIA	SA
SENEGAL	SN
SERBIA AND MONTENEGRO	CS
SEYCHELLES	SC
SIERRA LEONE	SL
SINGAPORE	SG
SLOVAKIA	SK
SLOVENIA	SI
SOLOMON ISLANDS	SB
SOMALIA	SO
SOUTH AFRICA	ZA
SOUTH GEORGIA AND THE SOUTH SANDWICH ISLANDS	GS
SPAIN	ES
SRI LANKA	LK
SUDAN	SD
SURINAME	SR
SVALBARD AND JAN MAYEN	SJ
SWAZILAND	SZ
SWEDEN	SE
SWITZERLAND	CH
SYRIAN ARAB REPUBLIC	SY
TAIWAN, PROVINCE OF CHINA	TW
TAJIKISTAN	TJ
TANZANIA, UNITED REPUBLIC OF	TZ
THAILAND	TH
TIMOR-LESTE	TL
TOGO	TG
TOKELAU	TK
TONGA	TO
TRINIDAD AND TOBAGO	TT
TUNISIA	TN
TURKEY	TR
TURKMENISTAN	TM
TURKS AND CAICOS ISLANDS	TC
TUVALU	TV
UGANDA	UG
UKRAINE	UA
UNITED ARAB EMIRATES	AE
UNITED KINGDOM	GB
UNITED STATES	US
UNITED STATES MINOR OUTLYING ISLANDS	UM
URUGUAY	UY
UZBEKISTAN	UZ
VANUATU	VU
VATICAN CITY STATE (HOLY SEE)	VA
VENEZUELA	VE
VIET NAM	VN
VIRGIN ISLANDS, BRITISH	VG

VIRGIN ISLANDS, US	VI
WALLIS AND FUTUNA	WF
WESTERN SAHARA	EH
YEMEN	YE
ZAIRE (CONGO, THE DEMOCRATIC REPUBLIC OF THE)	CD
ZAMBIA	ZM
ZIMBABWE	ZW

3.3.2.1.11.3 List of blocked countries

Set countries which you want to block and from which you do not want to receive messages. To add a country to **Blocked countries:** list, select it from the **Country code:** column and press **Add** button. To remove the country from **Blocked countries:** list, select the country code and press **Remove** button.

For list of specific country codes see List of home countries 48 topic.

3.3.2.1.11.4 List of blocked charsets

Set the char-sets you want to block. Messages in these char-sets will not be received. To add a char-set, select it from the **Charsets:** column and press **Add** button. This will move the char-set to the **Blocked charsets:** column. To remove the char-set from **Blocked charsets:** column, select the char-set code and press **Remove** button.

While adding a char-set to blocked char-sets, you can specify your own value for SPAM score for this particular char-set. Default is 100. You can define score for each char-set separately.

3.3.2.1.12 Log files

Turn on detailed logging - Enables increased verbose logging.

Output rerouting files: - Redirects log output file to the directory specified in this field. Press **...** button to browse for directory instead of typing it it manually.

3.3.2.1.13 Statistics

Turn on statistical data logging - Logs IP's, Domains, URL's, suspicious words, etc. to the conf file system. Logs can be automatically uploaded to antispam engine's analysis servers. The logs can be converted to plain text for viewing.

- **Send statistical data for analysis** - Launches a thread to automatically upload statistics files to antispam engine's analysis servers.
- **Analysis server address:** - URL where statistics files will be uploaded.

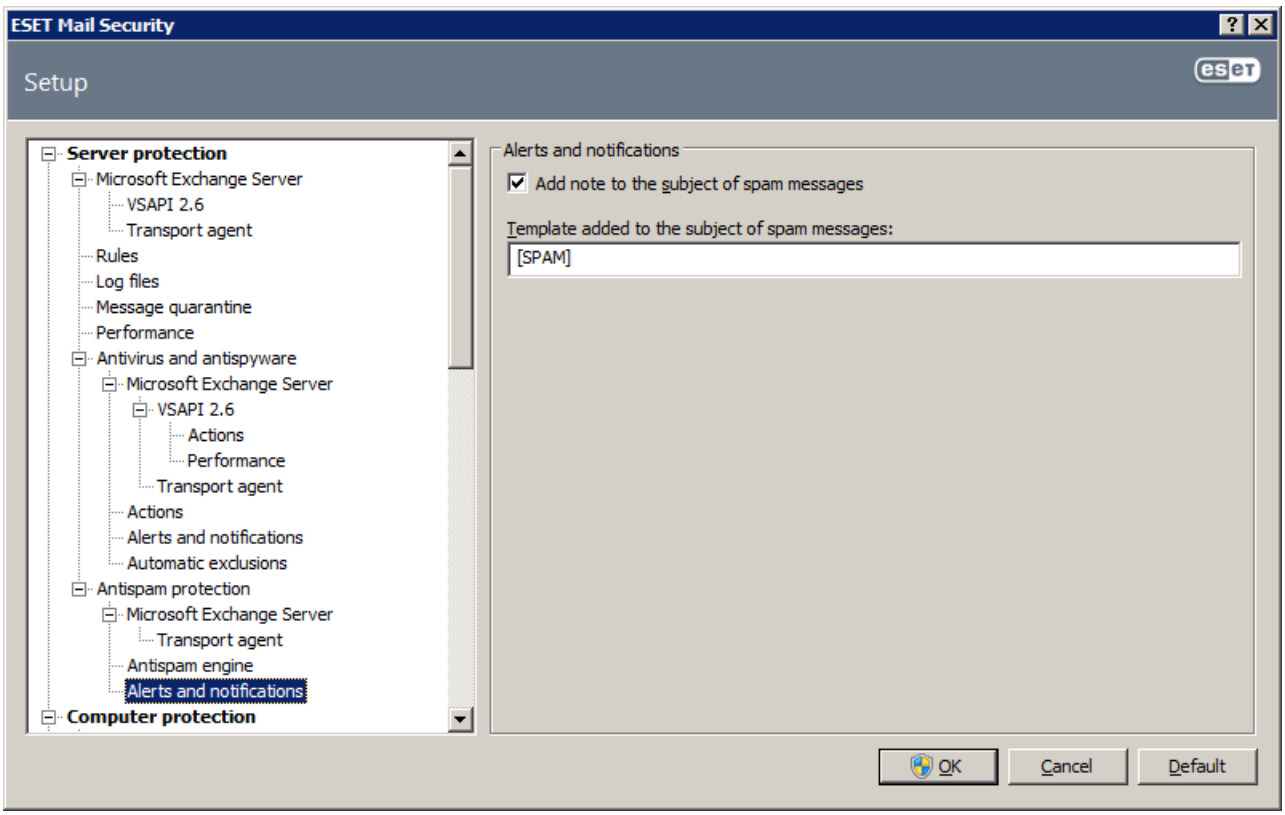
3.3.2.1.14 Options

Automatic configuration: - Sets options based on user-inputted system, performance, and resource requirements.

Create configuration file - Creates *antispam.cfg* file wich contains antispam engine configuration. It can be found in C:*ProgramData\ESET\ESET Mail Security\ServerAntispam* (Windows Server 2008) or C:*Documents and Settings\All Users\Application Data\ESET\ESET Mail Security\ServerAntispam* (Windows Server 2000 and 2003).

3.3.3 Alerts and notifications

Each email scanned by ESET Mail Security and marked as spam can be flagged by appending a notification tag to the email subject. By default, the tag is [*SPAM*], although it can be a user-defined string.



NOTE: You can also use system variables when adding a template to the message subject.

3.4 FAQ

Q: After installing EMSX with Antispam, emails stopped being delivered into mailboxes.

A: If Greylisting is enabled, this is normal behavior. In the first hours of full operation emails may arrive with several hours of delay. If the issue continues for a longer period, we recommend you turn off (or reconfigure) Greylisting.

Q: When the VSAPI scans email attachments, does it also scan email message bodies?

A: In Microsoft Exchange Server 2000 SP2 and later, the VSAPI scans email message bodies as well.

Q: Why does message scanning continue after the VSAPI option has been disabled?

A: Changes to VSAPI settings run asynchronously, meaning the modified VSAPI settings have to be called by the Microsoft Exchange Server to go into effect. This cyclic process runs in intervals of approximately one minute. The same applies to all other VSAPI settings.

Q: Can VSAPI remove an entire message containing an infected attachment?

A: Yes, VSAPI can remove the entire message. However, it is necessary to select the **Delete whole message** option in the **Actions** section of the VSAPI settings first. This option is available in Microsoft Exchange Server 2003 and later. Older versions of Microsoft Exchange Server do not support removal of entire messages.

Q: Is outgoing email also scanned by VSAPI for viruses?

A: Yes, VSAPI scans outgoing emails unless you have configured an SMTP server in your mail client that is different from your Microsoft Exchange Server. This feature is applied in Microsoft Exchange Server 2000 Service Pack 3 and later.

Q: Is it possible to add a notification tag text via VSAPI to each scanned message, in the same manner as the Transport agent?

A: Adding text to messages scanned by VSAPI is not supported in Microsoft Exchange Server.

Q: Sometimes I cannot open a particular email in Microsoft Outlook. Why is that?

A: The Action to take if cleaning not possible option in your VSAPI settings in the **Actions** section is most likely set to **Block** or you have created a rule that includes the **Block** action. Either of these settings will mark and block both infected messages and/or messages that fall under the aforementioned rule.

Q: What does the **Response time limit** item in the **Performance** section stand for?

A: If you have Microsoft Exchange Server 2000 SP2 or later, the value **Response time limit** represents the maximum time in seconds required to finish the VSAPI scanning of one thread. If the scan is not finished within this time limit, Microsoft Exchange Server will deny the client access to the email. Scanning will not be interrupted and after it is finished, every other attempt to access the file will be successful. If you have Microsoft Exchange Server 5.5 SP3 or SP4, the value will be expressed in milliseconds and represents the period after which the client will retry to access the file that had been previously inaccessible due to scanning..

Q: How long can the list of file types be in one rule?

A: The file extensions list can contain a maximum of 255 characters in a single rule.

Q: I have enabled the **Background scanning** option in VSAPI. Until now, messages on Microsoft Exchange Server were always scanned after each virus signature database update. This did not happen after the last update. Where is the problem?

A: The decision to scan all messages immediately or at the user's attempt to access a message depends on several factors, including server load, CPU time required to scan all messages in bulk and the total number of messages. The Microsoft Exchange Server will scan every message before it reaches the client's inbox.

Q: Why did the rule counter increase by more than one after receiving a single message?

A:The rules are checked against a message when it is processed by transport agent (TA) or VSAPI. When both TA and VSAPI are enabled and the message matches the rule conditions, the rule counter may increase by 2 or more. VSAPI accesses the parts of the message individually (body, attachment) meaning the rules are consequently applied to each part individually. Furthermore, rules can be applied during a background scan (e.g. repeated mailbox-store scan after a virus signature database update), which can increase the rule counter.

Q: Is ESET Mail Security 4 for Microsoft Exchange Server compatible with Intelligent Message Filter?

A: Yes, ESET Mail Security 4 for Microsoft Exchange Server (EMSX) is compatible with Intelligent Message Filter (IMF). The processing of emails in the case that message is evaluated as spam is as follows:

- If ESET Mail Security Antispam has the **Delete message** (or **Quarantine message**) option enabled the action will be executed regardless of the action set in Microsoft Exchange IMF.

- If ESET Mail Security Antispam has the **No action** set, the Microsoft Exchange IMF settings will be used and the relevant action executed (e.g. Delete, Reject, Archive...). **Write spam confidence level (SCL) to scanned messages based on spam score** option (in **Server protection > Microsoft Exchange Server > Transport agent**) must be enabled in order for this feature to work effectively.

Q: How do I setup ESET Mail Security to move unsolicited emails into the user-defined Microsoft Outlook spam folder?

A: ESET Mail Security default settings cause Microsoft Outlook to store unwanted email in the **Junk E-mail** folder. To allow for this to work deselect the **Write spam score to the header of scanned email** option (under **F5 > Server protection > Antispam protection > Microsoft Exchange Server > Transport agent**). If you want the unwanted email to be stored in a different folder, please read the following instructions:

1) In ESET Mail Security:

   - go to advanced setup tree **F5**,

   - naviage to **Server protection** > **Antispam protection** > **Microsoft Exchange Server** > **Transport agent**

   - select **Retain message** from the **Action to take on spam messages** drop-down menu

- deselect the check box **Write spam score to the header of scanned messages**

- navigate to **Alerts and notifications** under **Antispam protection**

- define a text tag that will be added to the subject field of unwanted messages, e.g. "[SPAM]", in the **Template added to the subject of spam messages** field

2) In Microsoft Outlook:

- setup a rule to ensure messages with a specific text in the subject ("[SPAM]") will be moved into the desired folder.

For more detailed instructions see this Knowledgebase article.

Q: In the antispam protection statistics many messages fall into the **Not scanned** category. What email is not scanned by the antispam protection?

A: The **Not scanned** category comprises of:

General:

- All messages that were scanned while the antispam protection has been disabled on any layers (mailserver, transport agent).

Microsoft Exchange Server 2003:

- All messages incoming from an **IP address**, that is in the IMF on the **Global Accept List**
- Messages from authenticated senders

Microsoft Exchange Server 2007:

- All messages sent within the organization (all will be scanned by antivirus protection)
- Messages from authenticated senders
- Messages from users configured to bypass antispam
- All messages sent into the mailbox, that has the **AntispamBypass** option enabled.
- All messages from senders on the **Safe Senders** list.

NOTE: Addresses defined in the whitelist and antispam engine settings do not fall into the **Not scanned** category, as this group is comprised solely of messages that were never processed by antispam.

Q: Users download messages to their email clients via POP3 (bypassing Microsoft Exchange server), but the mailboxes are stored on Microsoft Exchange Server. Will these emails be subject to antivirus and antispam scanning by ESET Mail Security?

A: In this type of configuration ESET Mail Security will scan the emails stored on the Microsoft Exchange Server only for the presence of viruses (via VSAPI). Antispam scanning will not be realized as this requires an SMTP server.

Q: Can I define the level of spam score the message has to attain to be classified as SPAM?

A: Yes you can set this limit in ESET Mail Security version 4.3 and higher (see chapter Antispam engine 38).

Q: Does the ESET Mail Security Antispam Protection module scan also messages that are downloaded via POP3 Connector?

A: ESET Mail Security does support standard Microsoft SBS POP3 Connector on SBS 2008, therefore messages downloaded via this POP3 Connector are scanned for the presence of spam. However, standard Microsoft SBS POP3 Connector on SBS 2003 is not supported. There also exist third party POP3 Connectors. Whether messages that are fetched via these third party POP3 Connectors are scanned for spam depends on how particular POP3 Connector is designed and how messages are being fetched via this POP3 Connector. For more information refer to the POP3 Connector and antispam 37 topic.

4. ESET Mail Security - Server protection

While providing Microsoft Exchange Server protection, ESET Mail Security has all of the necessary tools to ensure protection of the server itself (resident shield, web-access protection, email client protection and antispam).

4.1 Antivirus and antispyware protection

Antivirus protection guards against malicious system attacks by controlling file, email and Internet communication. If a threat with malicious code is detected, the Antivirus module can eliminate it by first blocking it, and then cleaning, deleting or moving it to quarantine.

4.1.1 Real-time file system protection

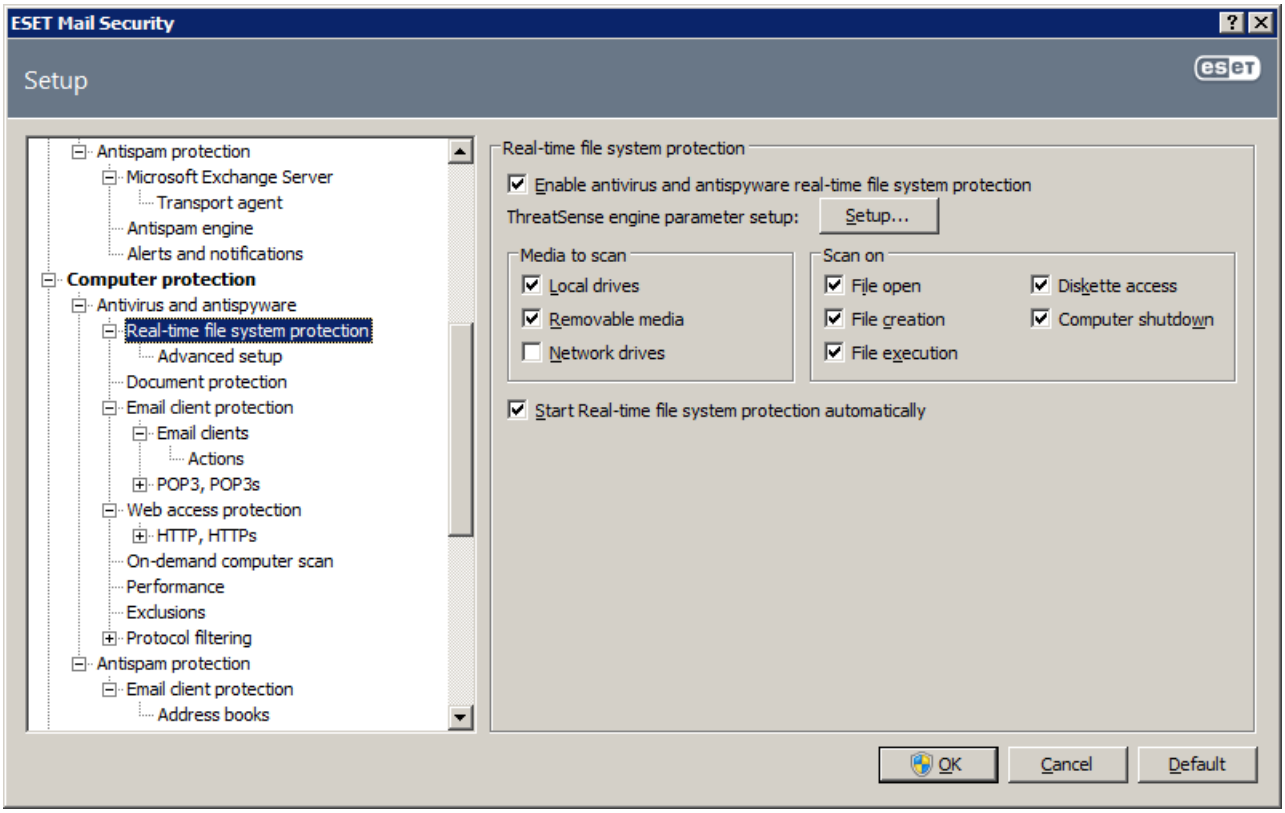
Real-time file system protection controls all antivirus-related events in the system. All files are scanned for malicious code at the moment they are opened, created or run on your computer. Real-time file system protection is launched at system startup.

4.1.1.1 Control setup

The Real-time file system protection checks all types of media, and control is triggered by various events. Using ThreatSense technology detection methods (as described in section ThreatSense engine parameter setup 72), real-time file system protection may vary for newly created files and existing files. For newly created files, it is possible to apply a deeper level of control.

To provide the minimum system footprint when using real-time protection, files which have already been scanned are not scanned repeatedly (unless they have been modified). Files are scanned again immediately after each virus signature database update. This behavior is configured using Smart optimization. If this is disabled, all files are scanned each time they are accessed. To modify this option, open the Advanced Setup window and click **Antivirus and antispyware** > **Realtime file system protection** from the Advanced Setup tree. Then click the **Setup...** button next to **ThreatSense engine parameter setup**, click **Other** and select or deselect the **Enable Smart optimization** option.

By default, Real-time protection launches at system startup and provides uninterrupted scanning. In special cases (e.g., if there is a conflict with another Real-time scanner), the real-time protection can be terminated by deselecting the **Start Real-time file system protection automatically** option.



4.1.1.1.1 Media to scan

By default, all types of media are scanned for potential threats.

Local drives – Controls all system hard drives

Removable media – Diskettes, USB storage devices, etc.

Network drives – Scans all mapped drives

We recommend that you keep the default settings and only modify them in specific cases, such as when scanning certain media significantly slows data transfers.

4.1.1.1.2 Scan on (Event-triggered scanning)

By default, all files are scanned upon opening, creation or execution. We recommend that you keep the default settings, as these provide the maximum level of real-time protection for your computer.

The **Diskette access** option provides control of the diskette boot sector when this drive is accessed. The **Computer shutdown** option provides control of the hard disk boot sectors during computer shutdown. Although boot viruses are rare today, we recommend that you leave these options enabled, as there is still the possibility of infection by a boot virus from alternate sources.

4.1.1.1.3 Advanced scan options

More detailed setup options can be found under **Computer protection** > **Antivirus and antispyware** > **Real-time system protection** > **Advanced setup**.

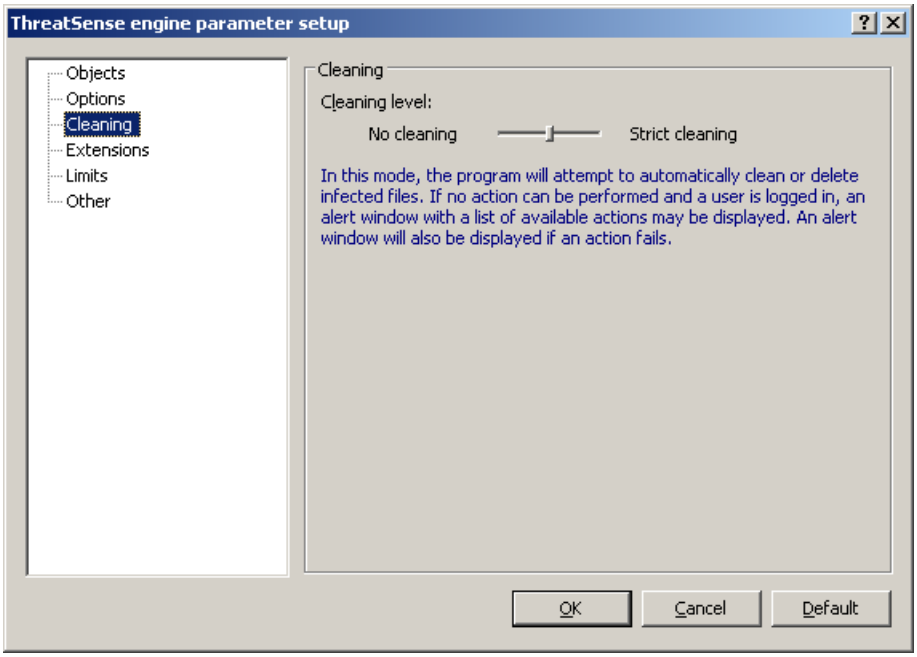
Additional ThreatSense parameters for newly created and modified files – The probability of infection in newly-created or modified files is comparatively higher than in existing files. That is why the program checks these files with additional scanning parameters. Along with common signature-based scanning methods, advanced heuristics are used, which greatly improves detection rates. In addition to newly-created files, scanning is also performed on self-extracting files (.sfx) and runtime packers (internally compressed executable files). By default, archives are scanned up to the 10th nesting level and are checked regardless of their actual size. To modify archive scan settings, deselect the Default archive scan settings option.

Additonal ThreatSense.Net parameters for executed files – By default, advanced heuristics are not used when files are executed. However, in some cases you may want to enable this option (by checking the **Advanced heuristics on file execution** option). Note that advanced heuristics may slow the execution of some programs due to increased system requirements.

4.1.1.2 Cleaning levels

Real-time protection has three cleaning levels. To select a cleaning level, click the **Setup...** button in the **Real-time file system protection** section and then click the **Cleaning** branch.

- The first level, **No cleaning**, displays an alert window with available options for each infiltration found. You must choose an action for each infiltration individually. This level is designed for more advanced users who know which steps to take in the event of an infiltration.
- The default level automatically chooses and performs a predefined action (depending on the type of infiltration). Detection and deletion of an infected file is signaled by a message located in the bottom right corner of the screen. Automatic actions are not performed when the infiltration is located within an archive (which also contains clean files) or when infected objects do not have a predefined action.
- The third level, **Strict cleaning**, is the most "aggressive" – all infected objects are cleaned. As this level could potentially result in the loss of valid files, we recommend that it be used only in specific situations.


ThreatSense engine parameter setup
Objects
Options
Cleaning
Extensions
Limits
Other
Cleaning
Cleaning level:
No cleaning
Strict cleaning
In this mode, the program will attempt to automatically clean or delete infected files. If no action can be performed and a user is logged in, an alert window with a list of available actions may be displayed. An alert window will also be displayed if an action fails.
OK
Cancel
Default

4.1.1.3 When to modify real-time protection configuration

Real-time protection is the most essential component of maintaining a secure system. Therefore, please be careful when modifying its parameters. We recommend that you only modify its parameters in specific cases. For example, if there is a conflict with a certain application or real-time scanner of another antivirus program.

After the installation of ESET Mail Security, all settings are optimized to provide the maximum level of system security for users. To restore the default settings, click the **Default** button located at the bottom-right of the **Real-time file system protection** window (**Advanced Setup** > **Antivirus and antispyware** > **Real-time file system protection**).

4.1.1.4 Checking real-time protection

To verify that real-time protection is working and detecting viruses, use a test file from eicar.com. This test file is a special harmless file detectable by all antivirus programs. The file was created by the EICAR company (European Institute for Computer Antivirus Research) to test the functionality of antivirus programs. The file eicar.com is available for download at http://www.eicar.org/download/eicar.com

NOTE: Before performing a real-time protection check, it is necessary to disable the firewall. If the firewall is enabled, it will detect the file and prevent test files from downloading.

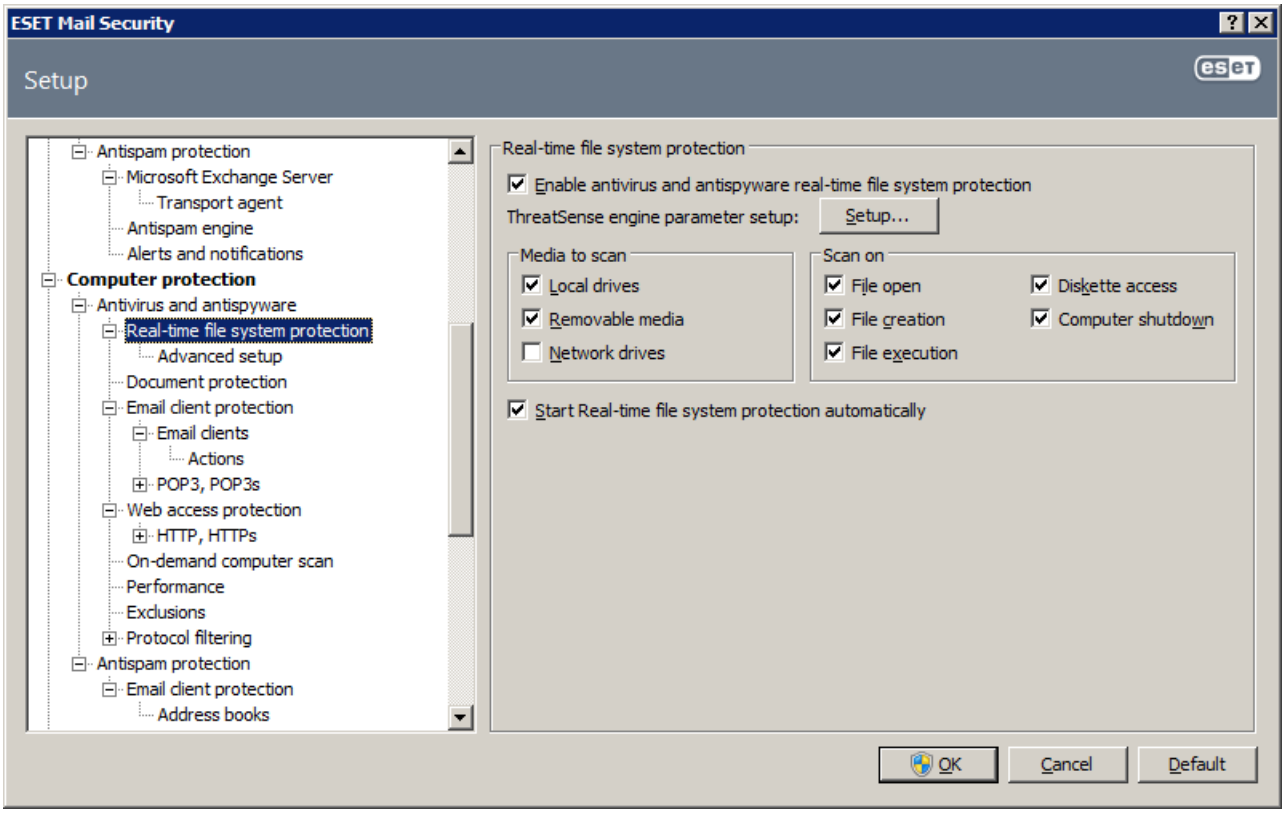
4.1.1.5 What to do if real-time protection does not work

In the next chapter, we describe problem situations that may arise when using real-time protection, and how to troubleshoot them.

Real-time protection is disabled

If real-time protection was inadvertently disabled by a user, it needs to be reactivated. To reactivate real-time protection, navigate to **Setup** > **Antivirus and antispyware** and click **Enable in the Real-time file system protection** section of the main program window.

If real-time protection is not initiated at system startup, it is probably due to the disabled option **Automatic real-time file system protection startup**. To enable this option, navigate to Advanced Setup (F5) and click **Real-time file system protection** in the Advanced Setup tree. In the **Advanced setup** section at the bottom of the window, make sure that the **Start Real-time file system protection automatically** checkbox is selected.



If Real-time protection does not detect and clean infiltrations

Make sure that no other antivirus programs are installed on your computer. If two real-time protection shields are enabled at the same time, they may conflict with each other. We recommend that you uninstall any other antivirus programs on your system.

Real-time protection does not start

If real-time protection is not initiated at system startup (and the **Start Real-time file system protection automatically** option is enabled), it may be due to conflicts with other programs. If this is the case, please consult ESET's Customer Care specialists.

4.1.2 Email client protection

Email protection provides control of email communication received through the POP3 protocol. Using the plug-in program for Microsoft Outlook, ESET Mail Security provides control of all communications from the email client (POP3, MAPI, IMAP, HTTP).

When examining incoming messages, the program uses all advanced scanning methods provided by the ThreatSense scanning engine. This means that detection of malicious programs takes place even before being matched against the virus signature database. Scanning of POP3 protocol communications is independent of the email client used.

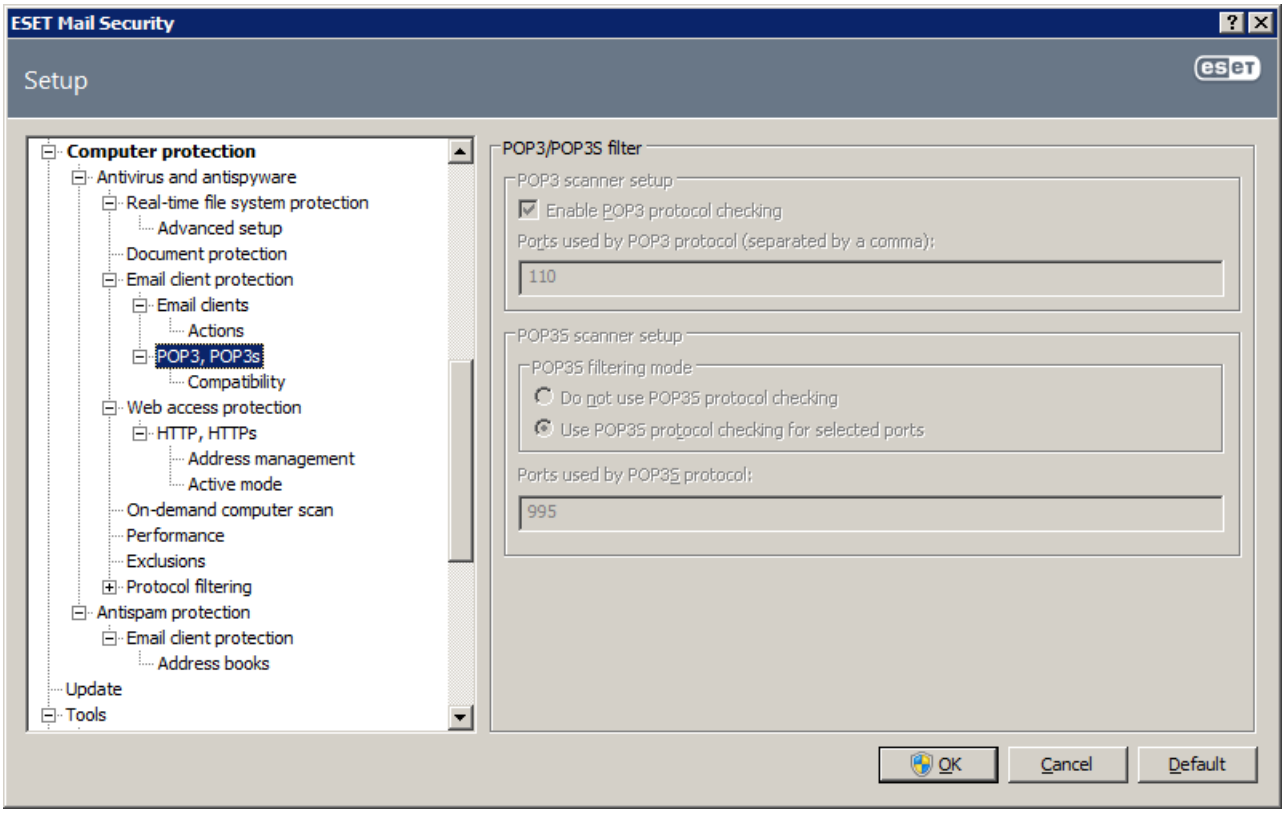
4.1.2.1 POP3 checking

The POP3 protocol is the most widespread protocol used to receive email communication in an email client application. ESET Mail Security provides protection for this protocol regardless of the email client used.

The protection module providing this control is automatically initiated at system startup and is then active in memory. For the module to work correctly, please make sure it is enabled – POP3 checking is performed automatically with no need for reconfiguration of the email client. By default, all communication on port 110 is scanned, but other communication ports can be added if necessary. Port numbers must be delimited by a comma.

Encrypted communication is not controlled.

To be able to use the POP3/POP3S filtering you need to enable Protocol filtering first. If the POP3/POP3S options are grayed out, navigate to **Computer protection** > **Antivirus and antispyware** > **Protocol filtering** from within the advanced setup tree and check **Enable application protocol content filtering**. See the Protocol filtering section for more details on filtering and configuration.



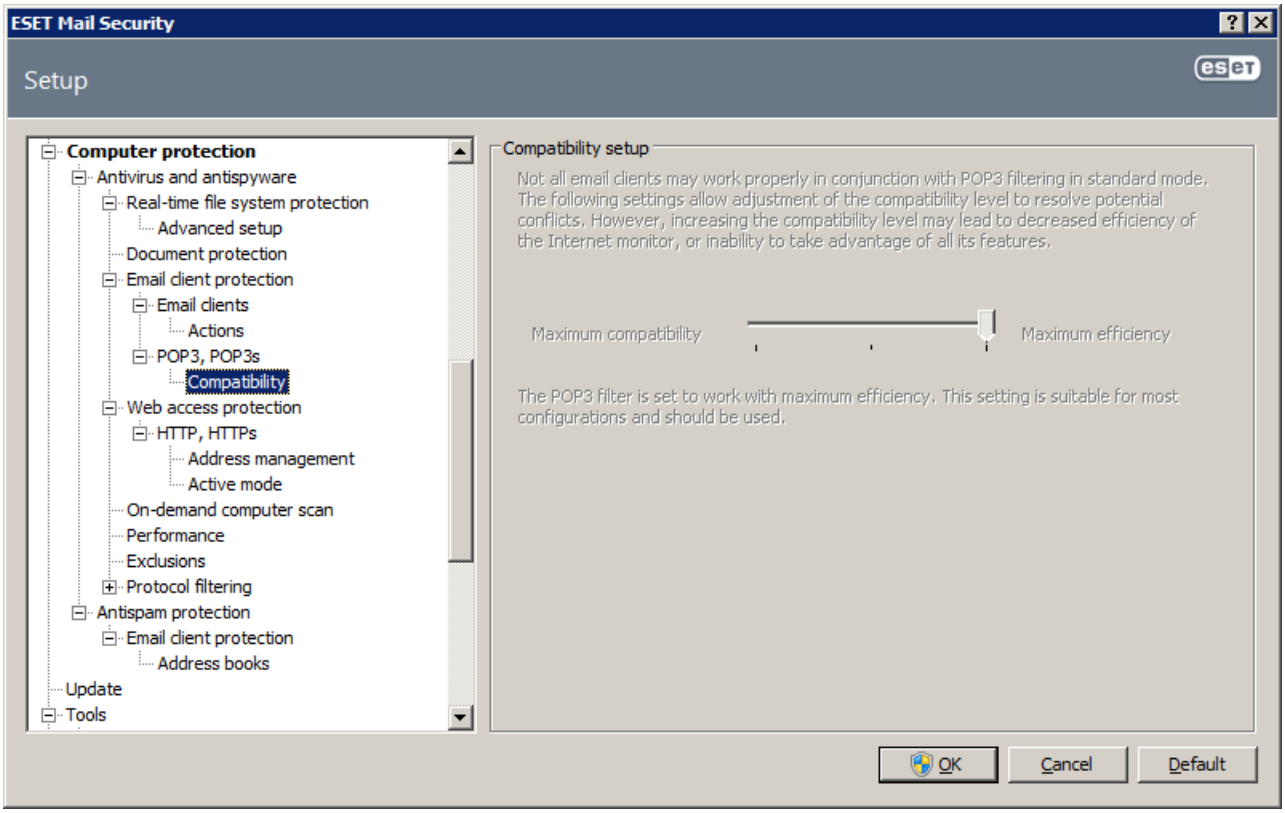
4.1.2.1.1 Compatibility

Certain email programs may experience problems with POP3 filtering (e.g., if receiving messages with a slow Internet connection, timeouts may occur due to checking). If this is the case, try modifying the way control is performed. Decreasing the control level may improve the speed of the cleaning process. To adjust the control level of POP3 filtering, from the Advanced Setup tree, navigate to **Antivirus and antispyware** > **Email protection** > **POP3, POP3s** > **Compatibility**.

If **Maximum efficiency** is enabled, infiltrations are removed from infected messages and information about the infiltration is inserted before the original email subject (the options **Delete** or **Clean** must be activated, or **Strict** or **Default** cleaning level must be enabled).

Medium compatibility modifies the way messages are received. Messages are gradually sent to the email client. After the message is transferred, it will be scanned for infiltrations. The risk of infection increases with this level of control. The level of cleaning and the handling of tag messages (notification alerts which are appended to the subject line and body of emails) is identical to the maximum efficiency setting.

With the **Maximum compatibility** level, you are warned by an alert window which reports the receipt of an infected message. No information about infected files is added to the subject line or to the email body of delivered messages and infiltrations are not automatically removed – you must delete infiltrations from the email client.

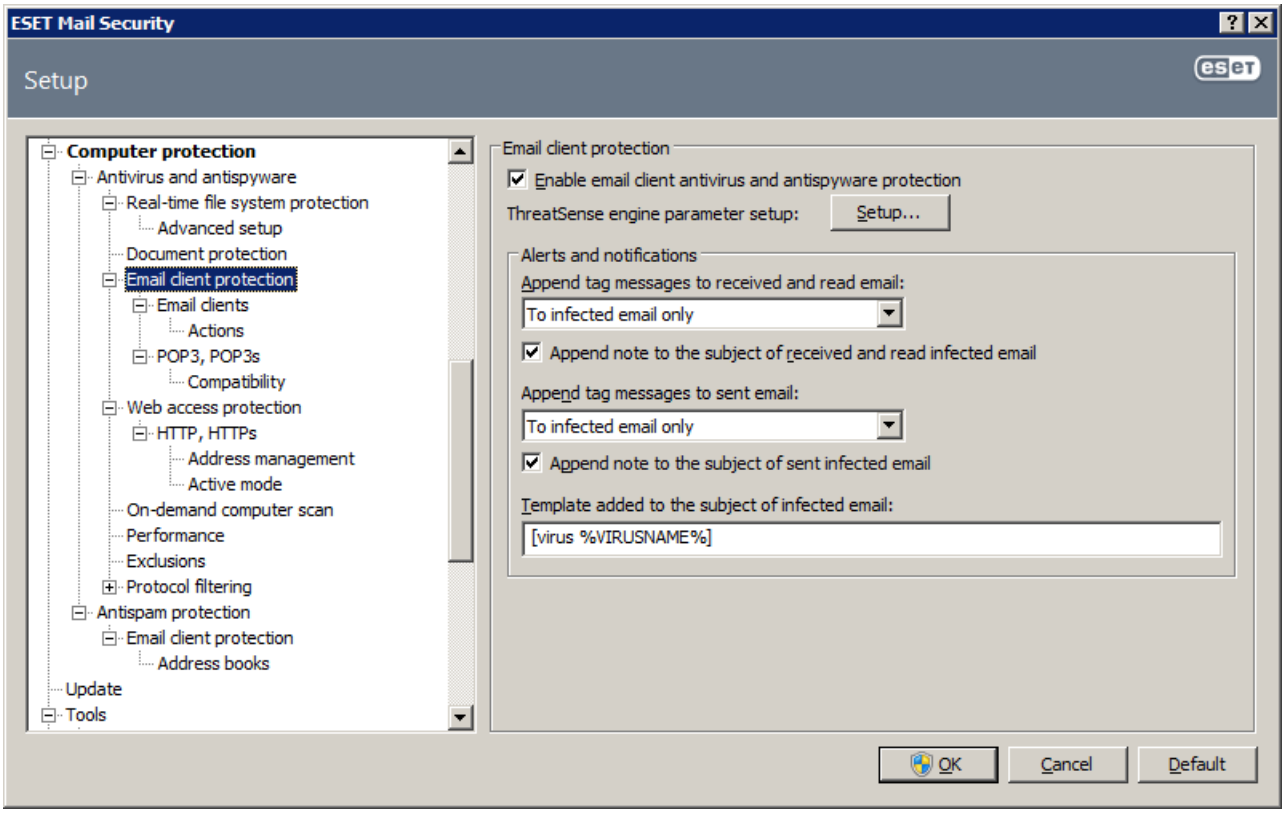

ESET Mail Security
Setup
Computer protection
Antivirus and antispyware
Real-time file system protection
Advanced setup
Document protection
Email client protection
Email clients
Actions
POP3, POP3s
Compatibility
Web access protection
HTTP, HTTPs
Address management
Active mode
On-demand computer scan
Performance
Exclusions
Protocol filtering
Antispam protection
Email client protection
Address books
Update
Tools
Compatibility setup
Not all email clients may work properly in conjunction with POP3 filtering in standard mode. The following settings allow adjustment of the compatibility level to resolve potential conflicts. However, increasing the compatibility level may lead to decreased efficiency of the Internet monitor, or inability to take advantage of all its features.
Maximum compatibility
Maximum efficiency
The POP3 filter is set to work with maximum efficiency. This setting is suitable for most configurations and should be used.
OK
Cancel
Default

4.1.2.2 Integration with email clients

Integration of ESET Mail Security with email clients increases the level of active protection against malicious code in email messages. If your email client is supported, this integration can be enabled in ESET Mail Security. If integration is activated, the ESET Mail Security toolbar is inserted directly into the email client, allowing for more efficient email protection. The integration settings are available through **Setup** > **Enter entire advanced setup tree...** > **Miscellaneous** > **Email client integration**. Email client integration allows you to activate integration with supported email clients. Email clients that are currently supported include Microsoft Outlook, Outlook Express, Windows Mail, Windows Live Mail and Mozilla Thunderbird.

Select the **Disable checking upon inbox content change** option if you are experiencing a system slowdown when working with your email client. Such a situation may take place when downloading email from Kerio Outlook Connector Store

Email protection is activated by clicking **Setup** > **Enter entire advanced setup tree...** > **Antivirus and antispyware** > **Email client protection** and selecting the **Enable email client antivirus and antispyware protection** option.



4.1.2.2.1 Appending tag messages to email body

Each email scanned by ESET Mail Security can be marked by appending a tag message to the subject or email body. This feature increases the level of credibility for the recipient and if an infiltration is detected, it provides valuable information about the threat level of a given email or sender.

The options for this functionality are available through **Advanced setup** > **Antivirus and antispyware** > **Email client protection**. You can select to **Append tag messages to received and read mail**, as well as **Append tag messages to sent mail**. You also have the ability to decide whether tag messages are appended to all scanned email, to infected email only, or not at all.

ESET Mail Security also allows you to append messages to the original subject of infected messages. To enable appending to the subject, select both the **Append note to the subject of received and read infected email** and **Append note to the subject of sent infected email** options.

The content of notifications can be modified in the **Template added to the subject of infected email** field. The previously mentioned modifications can help automate the process of filtering infected email, as it allows you to filter email with a specific subject (if supported in your email client) to a separate folder.

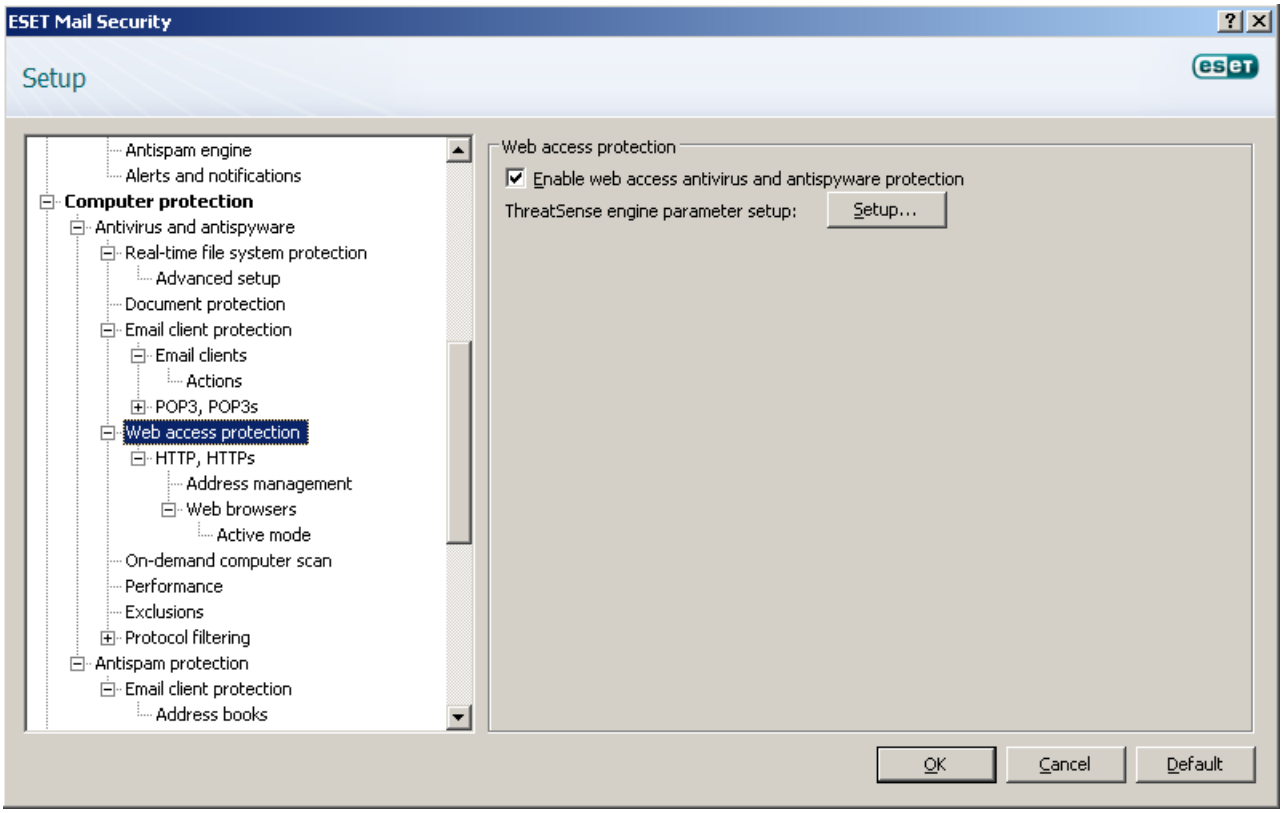
4.1.2.3 Removing infiltrations

If an infected email message is received, an alert window will display. The alert window shows the sender name, email and the name of the infiltration. In the lower part of the window the options **Clean**, **Delete** or **Leave** are available for the detected object. In almost all cases, we recommend that you select either **Clean** or **Delete**. In certain situations, if you wish to receive the infected file, select **Leave**.

If **Strict cleaning** is enabled, an information window with no options available for infected objects will displayed.

4.1.3 Web access protection

Internet connectivity is a standard feature in a personal computer. Unfortunately, it has also become the main medium for transferring malicious code. Because of this, it is essential that you carefully consider your Web access protection. We strongly recommend that the **Enable web access antivirus and antispyware protection** option is selected. This option is located in **Advanced Setup** (F5) > **Antivirus and antispyware** > **Web access protection**.

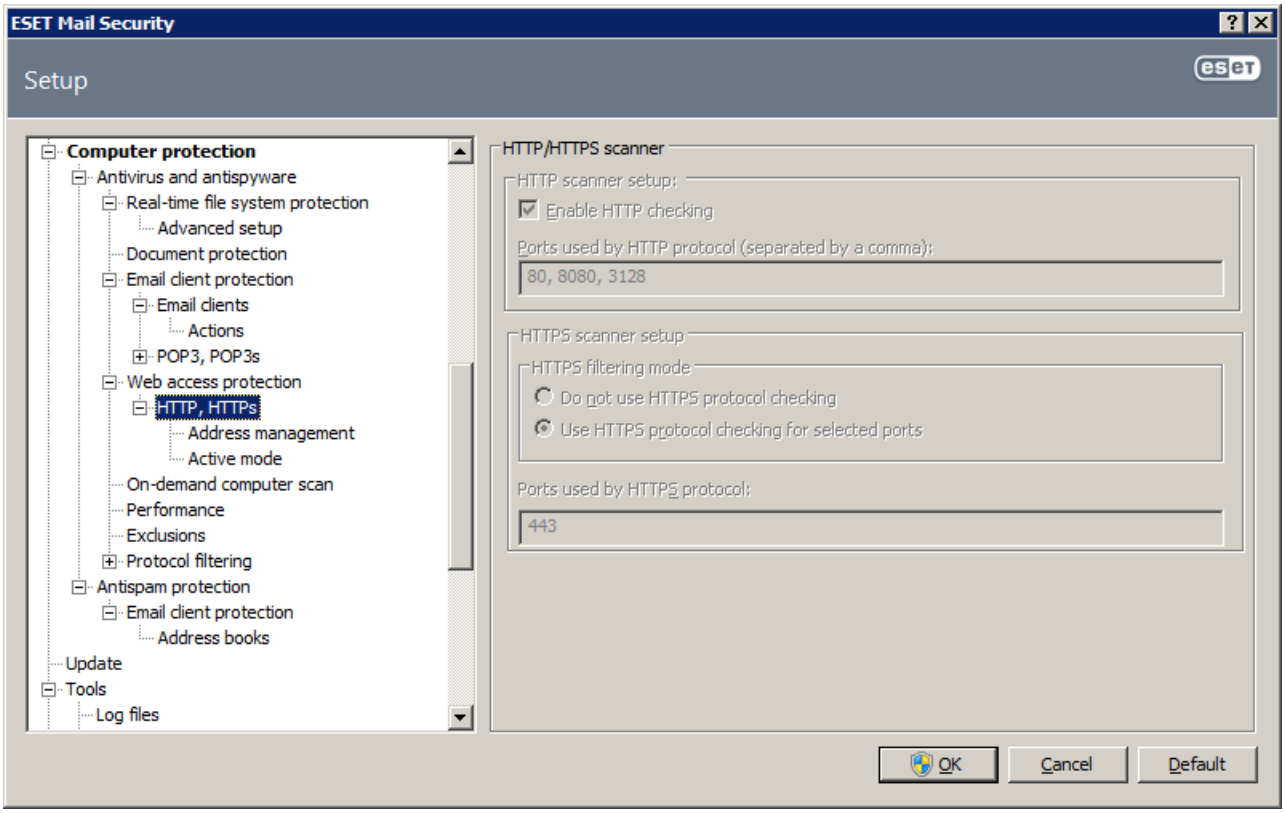


4.1.3.1 HTTP, HTTPs

Web access protection works by monitoring communication between Internet browsers and remote servers, and complies with HTTP (Hypertext Transfer Protocol) and HTTPs (encrypted communication) rules. By default, ESET Mail Security is configured to use the standards of most Internet browsers. However, the HTTP scanner setup options can be modified in **Advanced Setup** (F5) > **Antivirus and antispyware** > **Web access protection** > **HTTP, HTTPS**. In the main HTTP filter window, you can select or deselect the **Enable HTTP checking** option. You can also define the port numbers used for HTTP communication. By default, the port numbers 80, 8080 and 3128 are predefined. HTTPs checking can be performed in the following modes:

Do not use HTTPS protocol checking – Encrypted communication will not be checked

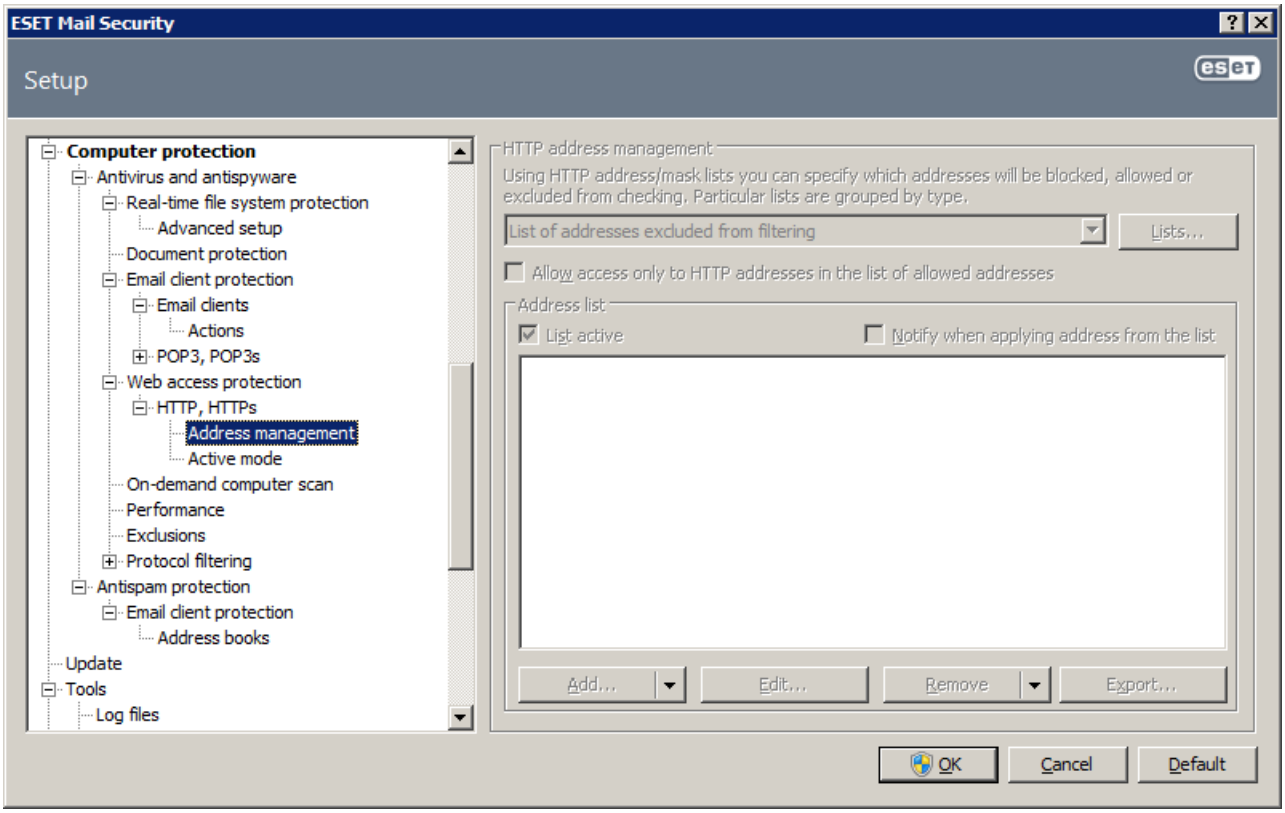
Use HTTPS protocol checking for selected ports – HTTPs checking only for ports defined in **Ports used by HTTPs protocol**



4.1.3.1.1 Address management

This section enables you to specify HTTP addresses to block, allow or exclude from checking. The buttons **Add...**, **Edit...**, **Remove** and **Export...** are used to manage the lists of addresses. Websites in the list of blocked addresses will not be accessible. Websites in the list of excluded addresses are accessed without being scanned for malicious code. If you select the **Allow access only to HTTP addresses in the list of allowed addresses** option, only addresses present in the list of allowed addresses will be accessible, while all other HTTP addresses will be blocked.

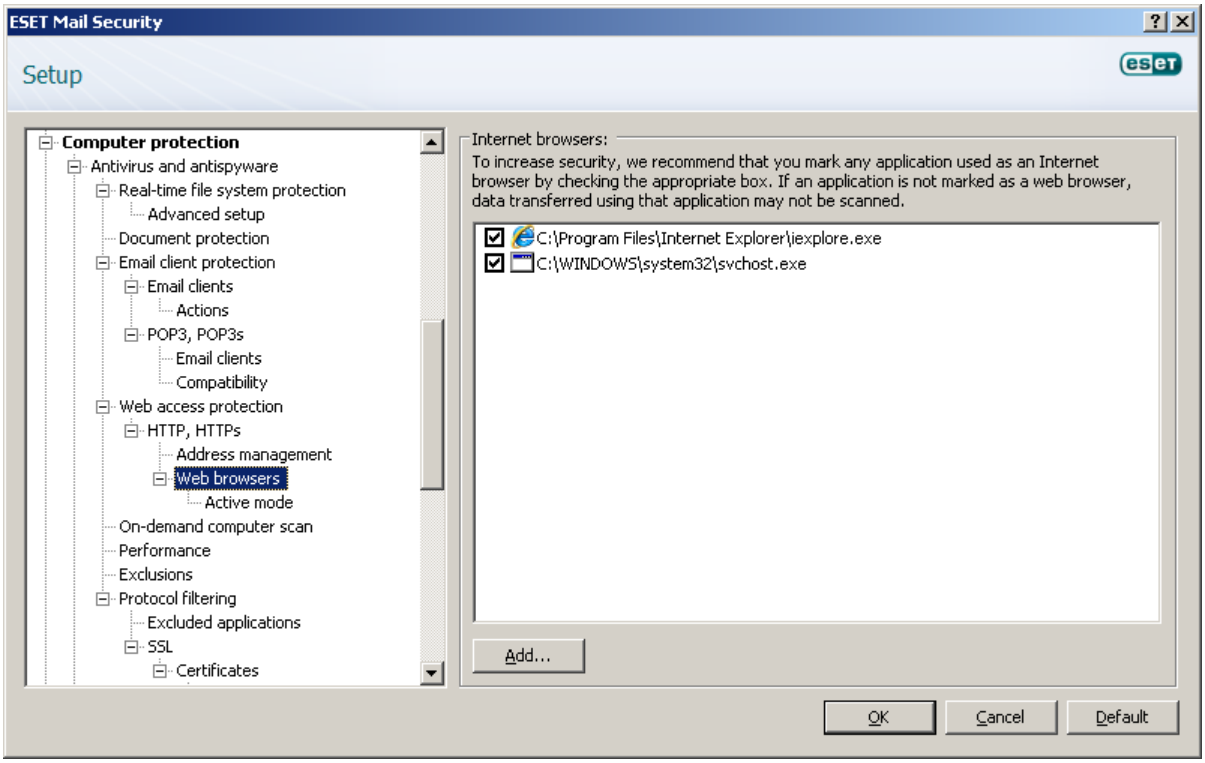
In all lists, the special symbols * (asterisk) and ? (question mark) can be used. The asterisk substitutes any character string, and the question mark substitutes any symbol. Particular care should be taken when specifying excluded addresses, because the list should only contain trusted and safe addresses. Similarly, it is necessary to ensure that the symbols * and ? are used correctly in this list. To activate a list, select the **List active** option. If you wish to be notified when entering an address from the current list, select **Notify when applying address from the list** option.



4.1.3.1.2 Active mode

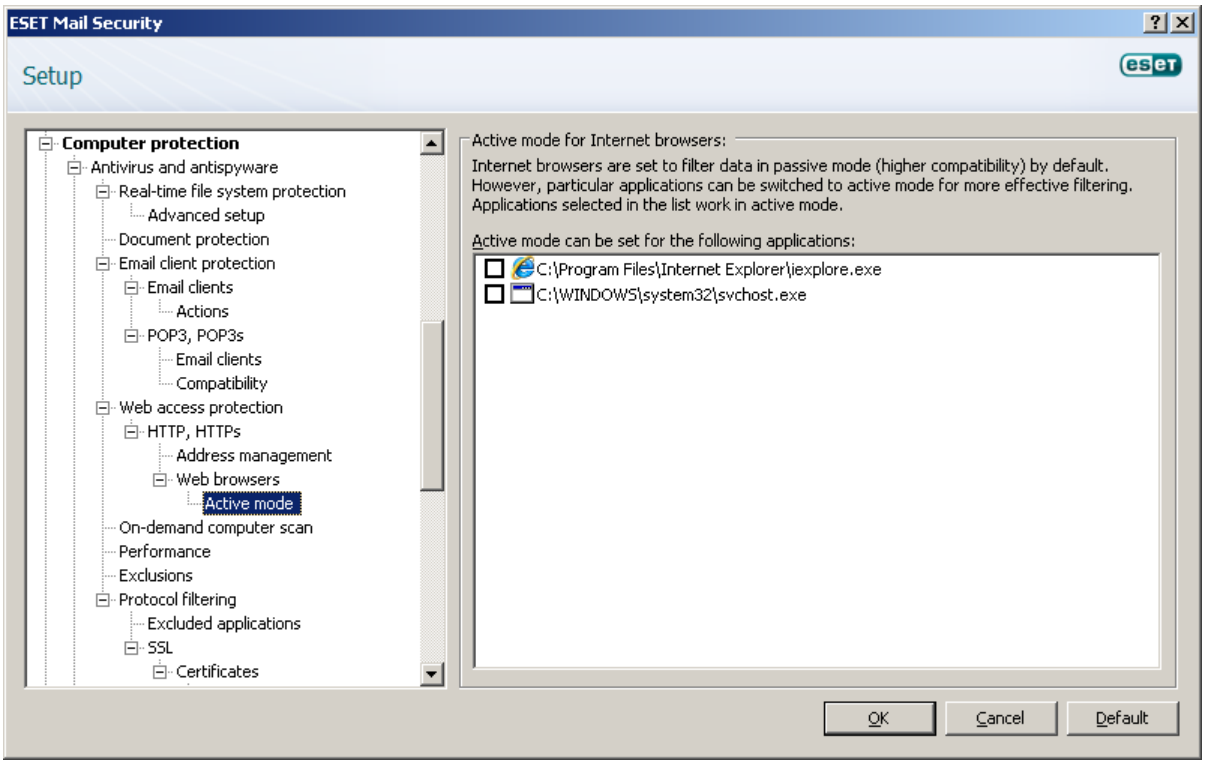
ESET Mail Security also contains the Web browsers feature, which allows you to define whether the given application is a browser or not. If an application is marked as a browser, all communication from this application is monitored regardless of the port numbers involved.

The Web browsers feature complements the HTTP checking feature, as HTTP checking only takes place on predefined ports. However, many Internet services utilize changing or unknown port numbers. To account for this, the Web browser feature can establish control of port communications regardless of the connection parameters.



The list of applications marked as web browsers is accessible directly from the **Web browsers** submenu of the **HTTP, HTTPs** branch. This section also contains the **Active mode** submenu, which defines the checking mode for Internet browsers.

Active mode is useful because it examines transferred data as a whole. If it is not enabled, communication of applications is monitored gradually in batches. This decreases the effectiveness of the data verification process, but also provides higher compatibility for listed applications. If no problems occur while using it, we recommend that you enable active checking mode by selecting the checkbox next to the desired application.



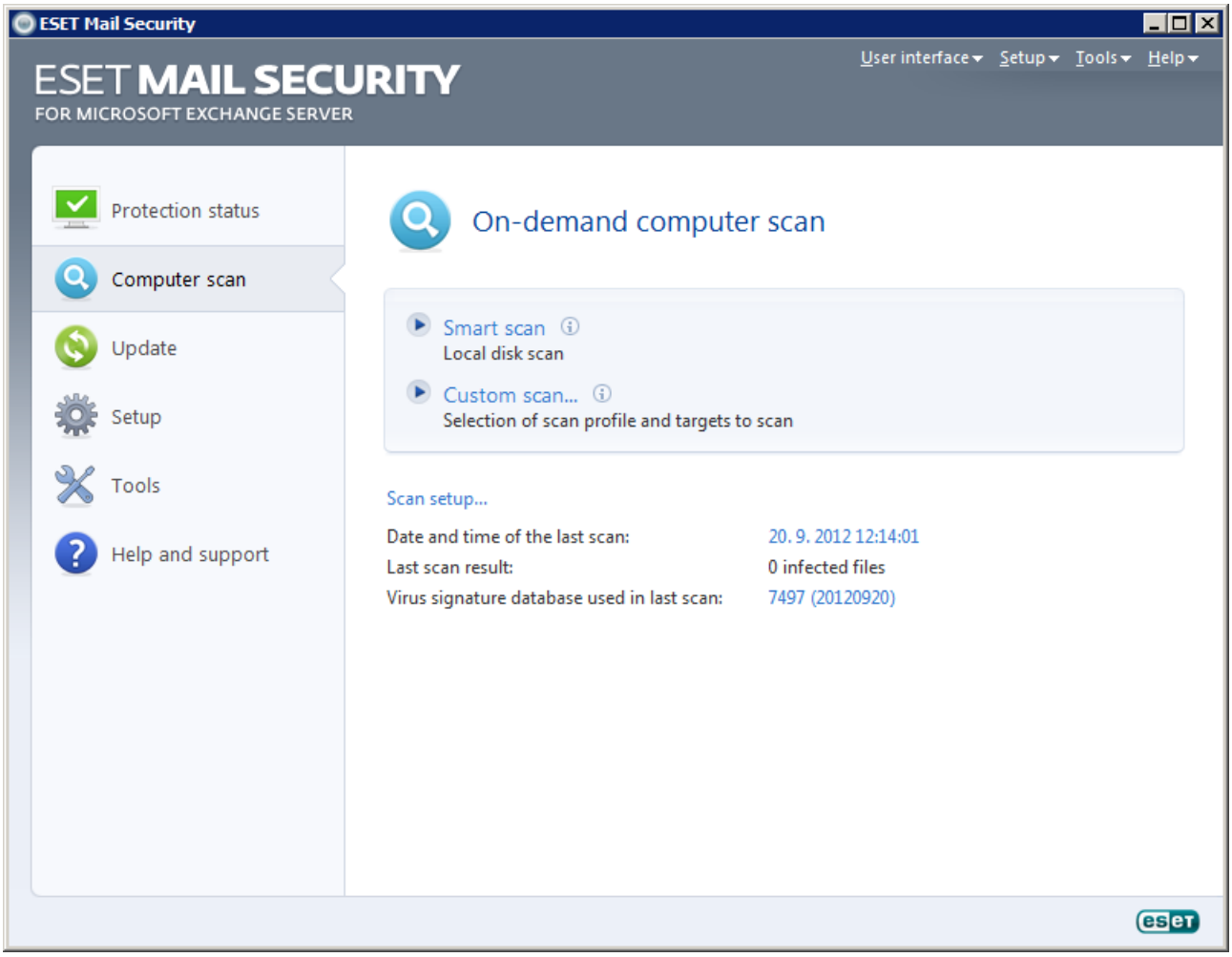
4.1.4 On-demand computer scan

If you suspect that your computer is infected (it behaves abnormally), run an On-demand computer scan to examine your computer for infiltrations. From a security point of view, it is essential that computer scans are not just run when an infection is suspected, but regularly as part of routine security measures. Regular scanning can detect infiltrations that were not detected by the real-time scanner when they were saved to the disk. This can happen if the real-time scanner was disabled at the time of infection, or if the virus signature database is not up-to-date.

We recommend that you run an On-demand computer scan at least once a month. Scanning can be configured as a scheduled task from **Tools** > **Scheduler**.

4.1.4.1 Type of scan

Two types of On-demand computer scan are available. **Smart scan** quickly scans the system with no need for further configuration of the scan parameters. **Custom scan...** allows you to select any of the predefined scan profiles, as well as choose specific scan targets.



4.1.4.1.1 Smart scan

Smart scan allows you to quickly launch a computer scan and clean infected files with no need for user intervention. Its main advantages are easy operation with no detailed scanning configuration. Smart scan checks all files on local drives and automatically cleans or deletes detected infiltrations. The cleaning level is automatically set to the default value. For more detailed information on types of cleaning, see section Cleaning 74.

4.1.4.1.2 Custom scan

Custom scan is an optimal solution if you wish to specify scanning parameters such as scan targets and scanning methods. The advantage of Custom scan is the ability to configure the parameters in detail. The configurations can be saved to user-defined scan profiles, which can be useful if scanning is repeatedly performed with the same parameters.

To select scan targets, select **Computer scan** > **Custom scan** and select an option from the **Scan targets** drop-down menu or select specific targets from the tree structure. A scan target can also be more precisely specified by entering the path to the folder or file(s) you wish to include. If you are only interested in scanning the system without additional cleaning actions, select the **Scan without cleaning** option. Furthermore, you can choose from three cleaning levels by clicking **Setup...** > **Cleaning**.

4.1.4.2 Scan targets

The Scan targets drop-down menu allows you to select files, folders and devices (disks) to be scanned for viruses.

By profile settings – Selects targets set in the selected scan profile

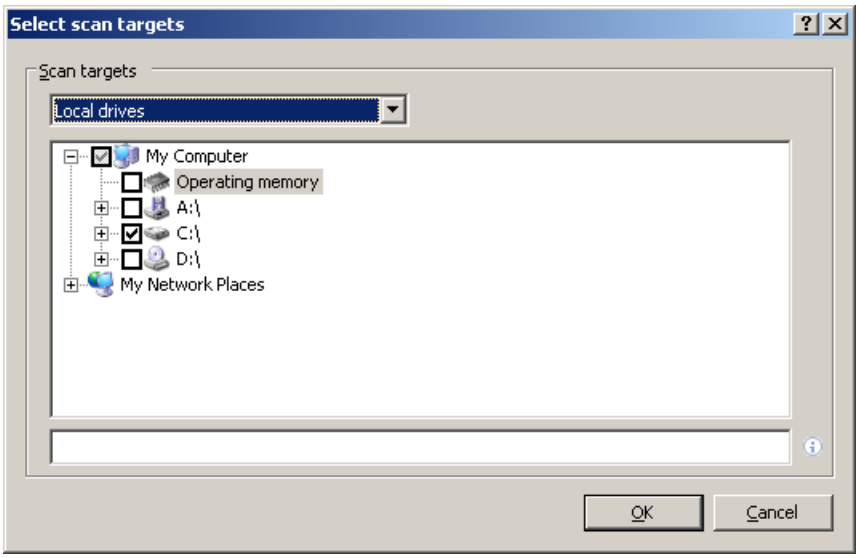
Removable media – Selects diskettes, USB storage devices, CD/DVD

Local drives – Selects all system hard drives

Network drives – Selects all mapped drives

No selection – Cancels all selections

A scan target can also be more precisely specified by entering the path to the folder or file(s) you wish to include in scanning. Select targets from the tree structure listing all devices available on the computer.

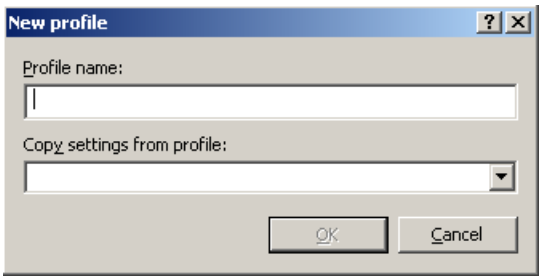


4.1.4.3 Scan profiles

Your preferred scan parameters can be saved for future scanning. We recommend that you create a different profile (with various scan targets, scan methods and other parameters) for each regularly used scan.

To create a new profile, open the Advanced Setup window (F5) and click **On-demand computer scan** > **Profiles...** The **Configuration profiles** window has a drop-down menu of existing scan profiles as well as the option to create a new one. To help you create a scan profile to fit your needs, see section ThreatSense engine parameters setup 72 for a description of each parameter of the scan setup.

EXAMPLE: Suppose that you want to create your own scan profile and the Smart scan configuration is partially suitable, but you don't want to scan runtime packers or potentially unsafe applications and you also want to apply **Strict cleaning**. From the **Configuration profiles** window, click the **Add...** button. Enter the name of your new profile in the **Profile name** field, and select **Smart scan** from the **Copy settings from profile**: drop-down menu. Then adjust the remaining parameters to meet your requirements.



4.1.4.4 Command Line

ESET Mail Security's antivirus module can be launched via the command line – manually (with the "ecls" command) or with a batch ("bat") file.

The following parameters and switches can be used while running the On-demand scanner from the command line:

General options:

– help	show help and quit
– version	show version information and quit
– base-dir = FOLDER	load modules from FOLDER
– quar-dir = FOLDER	quarantine FOLDER
– aind	show activity indicator

Targets:

– files	scan files (default)
– no-files	do not scan files
– boots	scan boot sectors (default)
– no-boots	do not scan boot sectorsk
– arch	scan archives (default)
– no-arch	do not scan archives
– max-archive-level = LEVEL	maximum archive nesting LEVEL
– scan-timeout = LIMIT	scan archives for LIMIT seconds at maximum. If the scanning time reaches this limit, the scanning of the archive is stopped and the scan will continue with the next file.
– max-arch-size=SIZE	scan only the first SIZE bytes in archives (default 0 = unlimited)
– mail	scan email files
– no-mail	do not scan email files
– sfx	scan self-extracting archives
– no-sfx	do not scan self-extracting archives
– rtp	scan runtime packers
– no-rtp	do not scan runtime packers
– exclude = FOLDER	exclude FOLDER from scanning
– subdir	scan subfolders (default)
– no-subdir	do not scan subfolders
– max-subdir-level = LEVEL	maximum subfolder nesting LEVEL (default 0 = unlimited)
– symlink	follow symbolic links (default)
– no-symlink	skip symbolic links
– ext-remove = EXTENSIONS	
– ext-exclude = EXTENSIONS	exclude EXTENSIONS delimited by colon from scanning

Methods:

– adware	scan for Adware/Spyware/Riskware
– no-adware	do not scan for Adware/Spyware/Riskware
– unsafe	scan for potentially unsafe applications
– no-unsafe	do not scan for potentially unsafe applications
– unwanted	scan for potentially unwanted applications
– no-unwanted	do not scan for potentially unwanted applications
– pattern	use signatures
– no-pattern	do not use signatures
– heur	enable heuristics
– no-heur	disable heuristics
– adv-heur	enable advanced heuristics
– no-adv-heur	disable advanced heuristics

Cleaning:

– action = ACTION	perform ACTION on infected objects. Available actions: none, clean, prompt
– quarantine	copy infected files to Quarantine (supplements ACTION)
– no-quarantine	do not copy infected files to Quarantine

Logs:

– log-file=FILE	log output to FILE
– log-rewrite	overwrite output file (default – append)
– log-all	log also clean files
– no-log-all	do not log clean files (default)

Possible exit codes of the scan:

0	– no threat found
1	– threat found but not cleaned
10	– some infected files remained
101	– archive error
102	– access error
103	– internal error

NOTE: Exit codes greater than 100 mean that the file was not scanned and thus can be infected.

4.1.5 Performance

In this section, you can set the number of ThreatSense scan engines that will be used for virus scanning. More ThreatSense scan engines on multiprocessor machines can increase the scanning rate. Acceptable value is 1-20.

If there are no other restrictions, our recommendation is to increase the number of ThreatSense scan engines in the Advanced settings window (F5) under **Computer protection** > **Antivirus and antispyware** > **Performance**, according to this formula: *number of ThreatSense scan engines = (number of physical CPUs x 2) + 1*. Also, the *number of scan threads* should be equal to the *number of ThreatSense scan engines*. You can configure the number of scan threads under **Server protection** > **Antivirus and antispyware** > **Microsoft Exchange Server** > **VSAPI** > **Performance**. Here is an example:

Let's say you have a server with 4 physical CPUs. For the best performance, according to formula above, you should have 9 scan threads and 9 scan engines.

NOTE: We recommend that you set the number of scan threads equal to the number of ThreatSense scan engines used. It will have no effect on performance if you use more scan threads than scan engines.

NOTE: Changes made here will be applied only after restart.

4.1.6 Protocol filtering

Antivirus protection, for the POP3 and HTTP application protocols, is provided by the ThreatSense scanning engine, which seamlessly integrates all advanced malware scanning techniques. The control works automatically, regardless of the Internet browser or email client used. The following options are available for protocol filtering (if the **Enable application protocol content filtering** option is selected):

HTTP and POP3 ports - Limits scanning of communication to known HTTP and POP3 ports.

Applications marked as Internet browsers and email clients – Enable this option to only filter communication of applications marked as browsers (**Web access protection** > **HTTP, HTTPS** > **Web browsers**) and email clients (**Email client protection** > **POP3, POP3s** > **Email clients**).

Ports and applications marked as Internet browsers or email clients – Both ports and browsers are checked for malware.

NOTE: Starting with Windows Vista Service Pack 1 and Windows Server 2008, a new communication filtering method is used. As a result, the Protocol filtering section is not available.

4.1.6.1 SSL

ESET Mail Security enables you to check protocols encapsulated in SSL protocol. You can use various scanning modes for SSL protected communications using trusted certificates, unknown certificates, or certificates that are excluded from SSL-protected communication checking.

Always scan SSL protocol – Select this option to scan all SSL protected communications except communications protected by certificates excluded from checking. If a new communication using an unknown, signed certificate is established, you will not be notified about the fact and the communication will automatically be filtered. When you access a server with an untrusted certificate that is marked by you as trusted (it is added to the trusted certificates list), communication to the server is allowed and the content of the communication channel is filtered.

Ask about non-visited sites (exclusions can be set) - If you enter a new SSL protected site (with an unknown certificate), an action selection dialog is displayed. This mode enables you to create a list of SSL certificates that will be excluded from scanning.

Do not scan SSL protocol - If selected, the program will not scan communications over SSL.

If the certificate cannot be verified using the Trusted Root Certification Authorities store (**protocol filtering** > **SSL** > **Certificates**):

Ask about certificate validity – Prompts you to select an action to take.

Block communication that uses the certificate – Terminates connection to the site that uses the certificate.

If the certificate is invalid or corrupt (**protocol filtering** > **SSL** > **Certificates**):

Ask about certificate validity – Prompts you to select an action to take.

Block communication that uses the certificate – Terminates connection to the site that uses the certificate.

4.1.6.1.1 Trusted certificates

In addition to the integrated Trusted Root Certification Authorities store where ESET Mail Security stores trusted certificates, you can create a custom list of trusted certificates that can be viewed in **Advanced Setup** (F5) > **Protocol filtering** > **SSL** > **Certificates** > **Trusted certificates**.

4.1.6.1.2 Excluded certificates

The Excluded certificates section contains certificates that are considered safe. The content of encrypted communications utilizing the certificates in the list will not be checked for threats. We recommend excluding only those web certificates that are guaranteed to be safe and the communication utilizing the certificates does not need to be checked.

4.1.7 ThreatSense engine parameters setup

ThreatSense is the name of the technology consisting of complex threat detection methods. This technology is proactive, which means it also provides protection during the early hours of the spread of a new threat. It uses a combination of several methods (code analysis, code emulation, generic signatures, virus signatures) which work in concert to significantly enhance system security. The scanning engine is capable of controlling several data streams simultaneously, maximizing the efficiency and detection rate. ThreatSense technology also successfully eliminates rootkits.

The ThreatSense technology setup options allow you to specify several scan parameters:

- File types and extensions that are to be scanned
- The combination of various detection methods
- Levels of cleaning, etc.

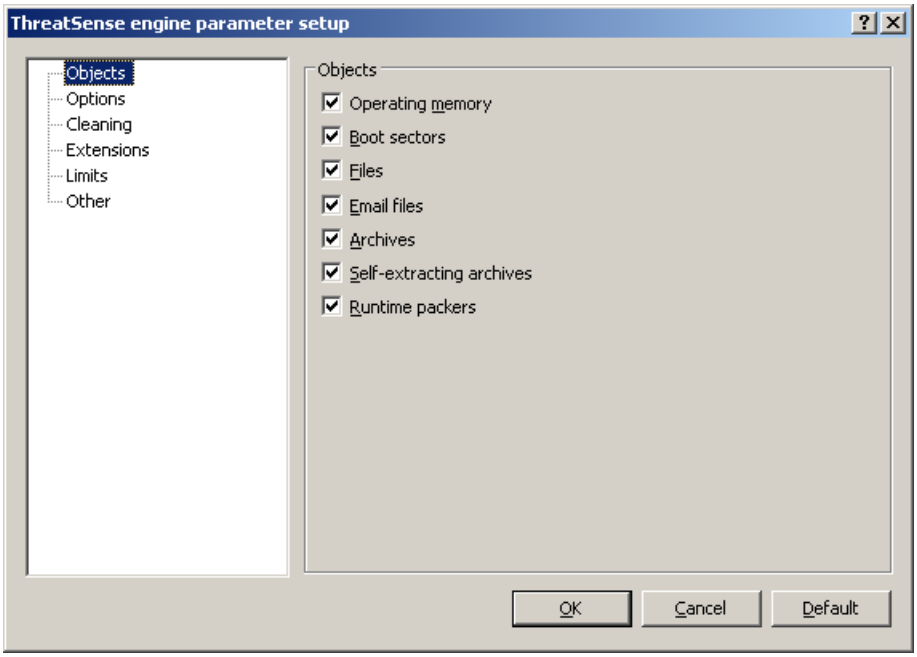
To enter the setup window, click the **Setup...** button located in any module's setup window which uses ThreatSense technology (see below). Different security scenarios could require different configurations. With this in mind, ThreatSense is individually configurable for the following protection modules:

- Real-time file system protection 56
- System startup file check
- Email protection 59
- Web access protection 63
- On-demand computer scan 66

The ThreatSense parameters are highly optimized for each module, and their modification can significantly influence system operation. For example, changing parameters to always scan runtime packers, or enabling advanced heuristics in the real-time file system protection module could result in a system slow-down (normally, only newly-created files are scanned using these methods). Therefore, we recommend that you leave the default ThreatSense parameters unchanged for all modules except On-demand computer scan.

4.1.7.1 Objects setup

The **Objects** section allows you to define which computer components and files will be scanned for infiltrations.



Operating memory – Scans for threats that attack the operating memory of the system.

Boot sectors – Scans boot sectors for the presence of viruses in the master boot record.

Files – Provides scanning for all common file types (programs, pictures, audio, video files, database files, etc.).

Email files – Scans special files where email messages are contained.

Archives – Provides scanning for files compressed in archives (.rar, .zip, .arj, .tar, etc.).

Self-extracting archives – Scans files which are contained in self-extracting archive files, but typically presented with an .exe file extension

Runtime packers – Runtime packers (unlike standard archive types) decompress in memory, in addition to standard static packers (UPX, yoda, ASPack, FGS, etc.).

NOTE: When a blue dot is shown next to a parameter, it means that current setting for this parameter differ from setting for other modules that also use ThreatSense. Since you can configure the same parameter differently for each module, this blue dot only reminds you that this same parameter is configured differently for other modules. If there isn't a blue dot, parameter for all the modules is configured the same way.

4.1.7.2 Options

In the **Options** section, you can select the methods to be used when scanning the system for infiltrations. The following options are available:

Signatures – Signatures can exactly and reliably detect and identify infiltrations by their name using virus signatures.

Heuristics – Heuristics use an algorithm that analyses the (malicious) activity of programs. The main advantage of heuristic detection is the ability to detect new malicious software which did not previously exist, or was not included in the list of known viruses (virus signatures database).

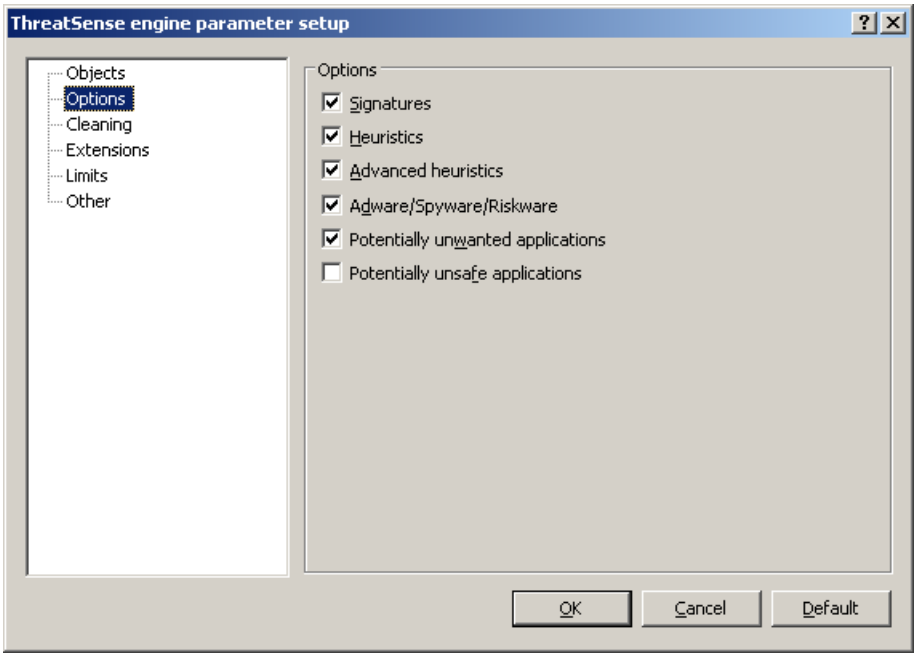
Advanced heuristics – Advanced heuristics comprise a unique heuristic algorithm, developed by ESET, optimized for detecting computer worms and trojan horses written in high-level programming languages. Due to advanced heuristics, the detection intelligence of the program is significantly higher.

Adware/Spyware/Riskware – This category includes software which collects various sensitive information about users without their informed consent. This category also includes software which displays advertising material.

Potentially unwanted applications – Potentially unwanted applications are not necessarily intended to be malicious, but may affect the performance of your computer in a negative way. Such applications usually require

consent for installation. If they are present on your computer, your system behaves differently (compared to the state before their installation). The most significant changes include unwanted pop-up windows, activation and running of hidden processes, increased usage of system resources, changes in search results, and applications communicating with remote servers.

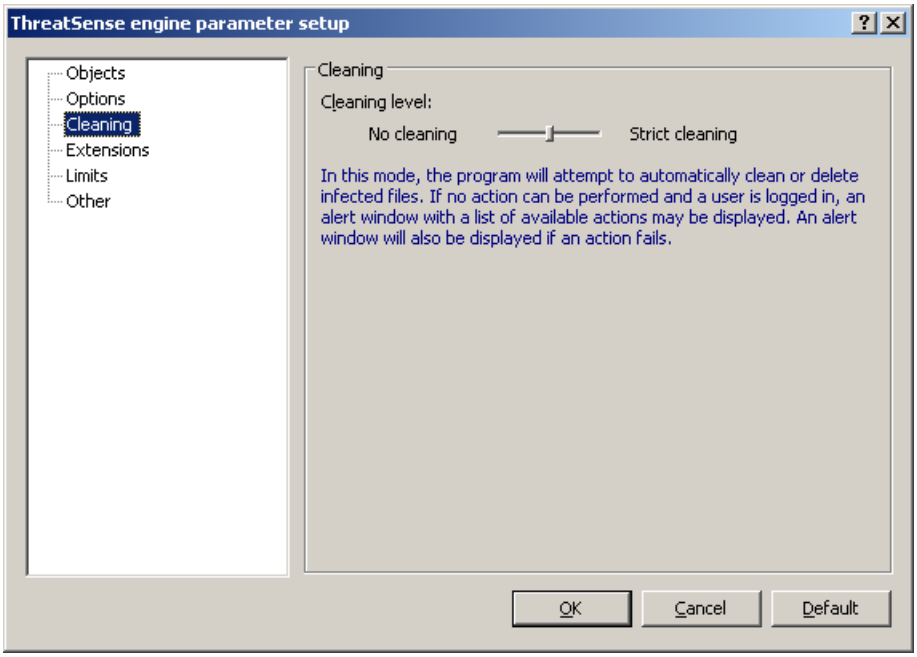
Potentially unsafe applications – Potentially unsafe applications is the classification used for commercial, legitimate software. It includes programs such as remote access tools, which is why this option is disabled by default.



NOTE: When a blue dot is shown next to a parameter, it means that current setting for this parameter differ from setting for other modules that also use ThreatSense. Since you can configure the same parameter differently for each module, this blue dot only reminds you that this same parameter is configured differently for other modules. If there isn't a blue dot, parameter for all the modules is configured the same way.

4.1.7.3 Cleaning

The cleaning settings determine the behavior of the scanner during the cleaning of infected files. There are 3 levels of cleaning:


ThreatSense engine parameter setup
Objects
Options
Cleaning
Extensions
Limits
Other
Cleaning
Cleaning level:
No cleaning
Strict cleaning
In this mode, the program will attempt to automatically clean or delete infected files. If no action can be performed and a user is logged in, an alert window with a list of available actions may be displayed. An alert window will also be displayed if an action fails.
OK
Cancel
Default

No cleaning – Infected files are not cleaned automatically. The program will display a warning window and allow you to choose an action.

Standard cleaning – The program will attempt to automatically clean or delete an infected file. If it is not possible

to select the correct action automatically, the program will offer a choice of follow up actions. The choice of follow-up actions will also be displayed if a predefined action could not be completed.

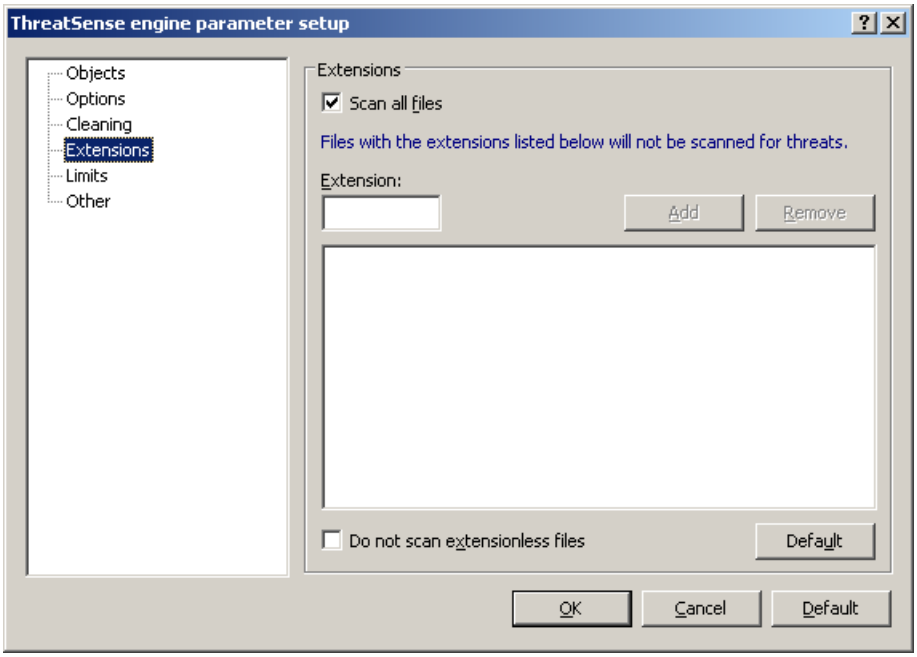
Strict cleaning – The program will clean or delete all infected files (including archives). The only exceptions are system files. If it is not possible to clean them, you will be offered an action to take in a warning window.

Warning: In the Default mode, the entire archive file is deleted only if all files in the archive are infected. If the archive also contains legitimate files, it will not be deleted. If an infected archive file is detected in Strict cleaning mode, the entire archive will be deleted, even if clean files are present.

NOTE: When a blue dot is shown next to a parameter, it means that current setting for this parameter differ from setting for other modules that also use ThreatSense. Since you can configure the same parameter differently for each module, this blue dot only reminds you that this same parameter is configured differently for other modules. If there isn't a blue dot, parameter for all the modules is configured the same way.

4.1.7.4 Extensions

An extension is part of the file name delimited by a period. The extension defines the type and content of the file. This section of the ThreatSense parameter setup lets you define the types of files to scan.



By default, all files are scanned regardless of their extension. Any extension can be added to the list of files excluded from scanning. If the **Scan all files** option is deselected, the list changes to show all currently scanned file extensions. Using the **Add** and **Remove** buttons, you can enable or prohibit scanning of desired extensions.

To enable scanning of files with no extension, select the **Scan extensionless files** option.

Excluding files from scanning is sometimes necessary if scanning certain file types prevents the program which is using the extensions from running properly. For example, it may be advisable to exclude the .edb, .eml and .tmp extensions when using Microsoft Exchange servers.

NOTE: When a blue dot is shown next to a parameter, it means that current setting for this parameter differ from setting for other modules that also use ThreatSense. Since you can configure the same parameter differently for each module, this blue dot only reminds you that this same parameter is configured differently for other modules. If there isn't a blue dot, parameter for all the modules is configured the same way.

4.1.7.5 Limits

The Limits section allows you to specify the maximum size of objects and levels of nested archives to be scanned:

Maximum object size: – Defines the maximum size of objects to be scanned. The given antivirus module will then scan only objects smaller than the size specified. We do not recommend changing the default value, as there is usually no reason to modify it. This option should only be changed by advanced users who have specific reasons for excluding larger objects from scanning.

Maximum scan time for object (sec.): – Defines the maximum time value for scanning an object. If a user-defined value has been entered here, the antivirus module will stop scanning an object when that time has elapsed, regardless of whether the scan has finished.

Archive nesting level: –Specifies the maximum depth of archive scanning. We do not recommend changing the default value of 10; under normal circumstances, there should be no reason to modify it. If scanning is prematurely terminated due to the number of nested archives, the archive will remain unchecked.

Maximum size of file in archive: – This option allows you to specify the maximum file size for files contained in archives (when they are extracted) that are to be scanned. If this causes scanning an archive to be prematurely terminated, the archive will remain unchecked.

NOTE: When a blue dot is shown next to a parameter, it means that current setting for this parameter differ from setting for other modules that also use ThreatSense. Since you can configure the same parameter differently for each module, this blue dot only reminds you that this same parameter is configured differently for other modules. If there isn't a blue dot, parameter for all the modules is configured the same way.

4.1.7.6 Other

Scan alternate data streams (ADS) – Alternate data streams (ADS) used by the NTFS file system are file and folder associations which are invisible from ordinary scanning techniques. Many infiltrations try to avoid detection by disguising themselves as alternative data streams.

Run background scans with low priority – Each scanning sequence consumes a certain amount of system resources. If you work with programs that place a high load on system resources, you can activate low priority background scanning and save resources for your applications.

Log all objects – If this option is selected, the log file will show all the scanned files, even those not infected.

Enable Smart optimization – Select this option so that files which have already been scanned are not scanned repeatedly (unless they have been modified). Files are scanned again immediately after each virus signature database update.

Preserve last access timestamp – Select this option to keep the original access time of scanned files instead of updating it (e.g., for use with data backup systems).

Scroll log – This option allows you to enable/disable log scrolling. If selected, information scrolls upwards within the display window.

Display notification about scan completion in a separate window – Opens a standalone window containing information about scan results.

NOTE: When a blue dot is shown next to a parameter, it means that current setting for this parameter differ from setting for other modules that also use ThreatSense. Since you can configure the same parameter differently for each module, this blue dot only reminds you that this same parameter is configured differently for other modules. If there isn't a blue dot, parameter for all the modules is configured the same way.

4.1.8 An infiltration is detected

Infiltrations can reach the system from various entry points; webpages, shared folders, via email or from removable computer devices (USB, external disks, CDs, DVDs, diskettes, etc.).

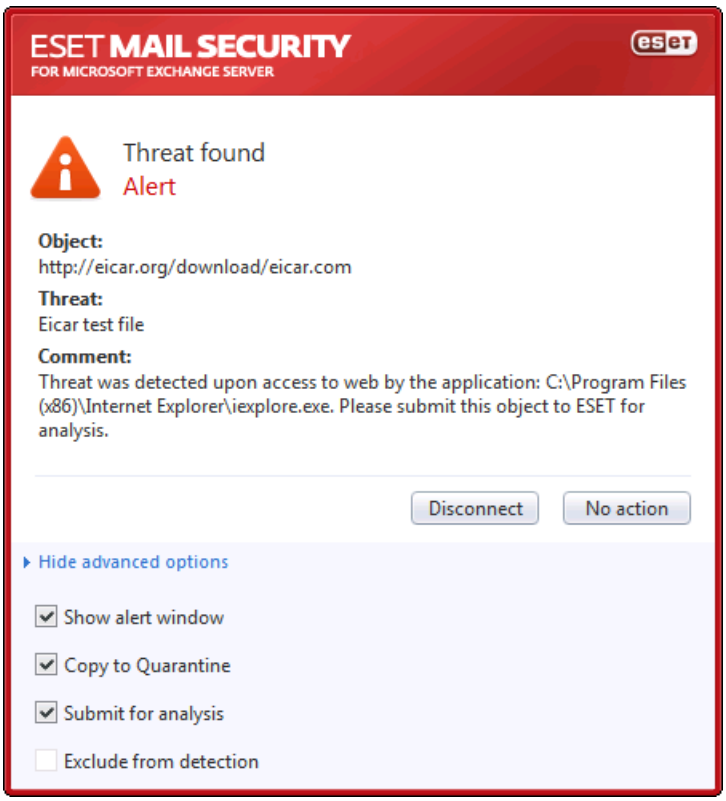
If your computer is showing signs of malware infection, e.g., it is slower, often freezes, etc., we recommend that you do the following:

- Open ESET Mail Security and click Computer scan
- Click **Smart scan** (for more information, see section Smart scan 67)
- After the scan has finished, review the log for the number of scanned, infected and cleaned files.

If you only wish to scan a certain part of your disk, click **Custom scan** and select targets to be scanned for viruses.

As a general example of how infiltrations are handled in ESET Mail Security, suppose that an infiltration is detected by the real-time file system monitor, which uses the Default cleaning level. It will attempt to clean or delete the file. If there is no predefined action to take for the real-time protection module, you will be asked to select an option in an alert window. Usually, the options **Clean**, **Delete** and **Leave** are available. Selecting **Leave** is not recommended, since the infected file(s) would be left untouched. The exception to this is when you are sure that the file is harmless and has been detected by mistake.

Cleaning and deleting – Apply cleaning if a file has been attacked by a virus which has attached malicious code to the file. If this is the case, first attempt to clean the infected file in order to restore it to its original state. If the file consists exclusively of malicious code, it will be deleted.



If an infected file is "locked" or in use by a system process, it will usually only be deleted after it is released (normally after a system restart).

Deleting files in archives – In the Default cleaning mode, the entire archive will be deleted only if it contains infected files and no clean files. In other words, archives are not deleted if they also contain harmless clean files. However, use caution when performing a Strict cleaning scan – with Strict cleaning the archive will be deleted if it contains at least one infected file, regardless of the status of other files in the archive.

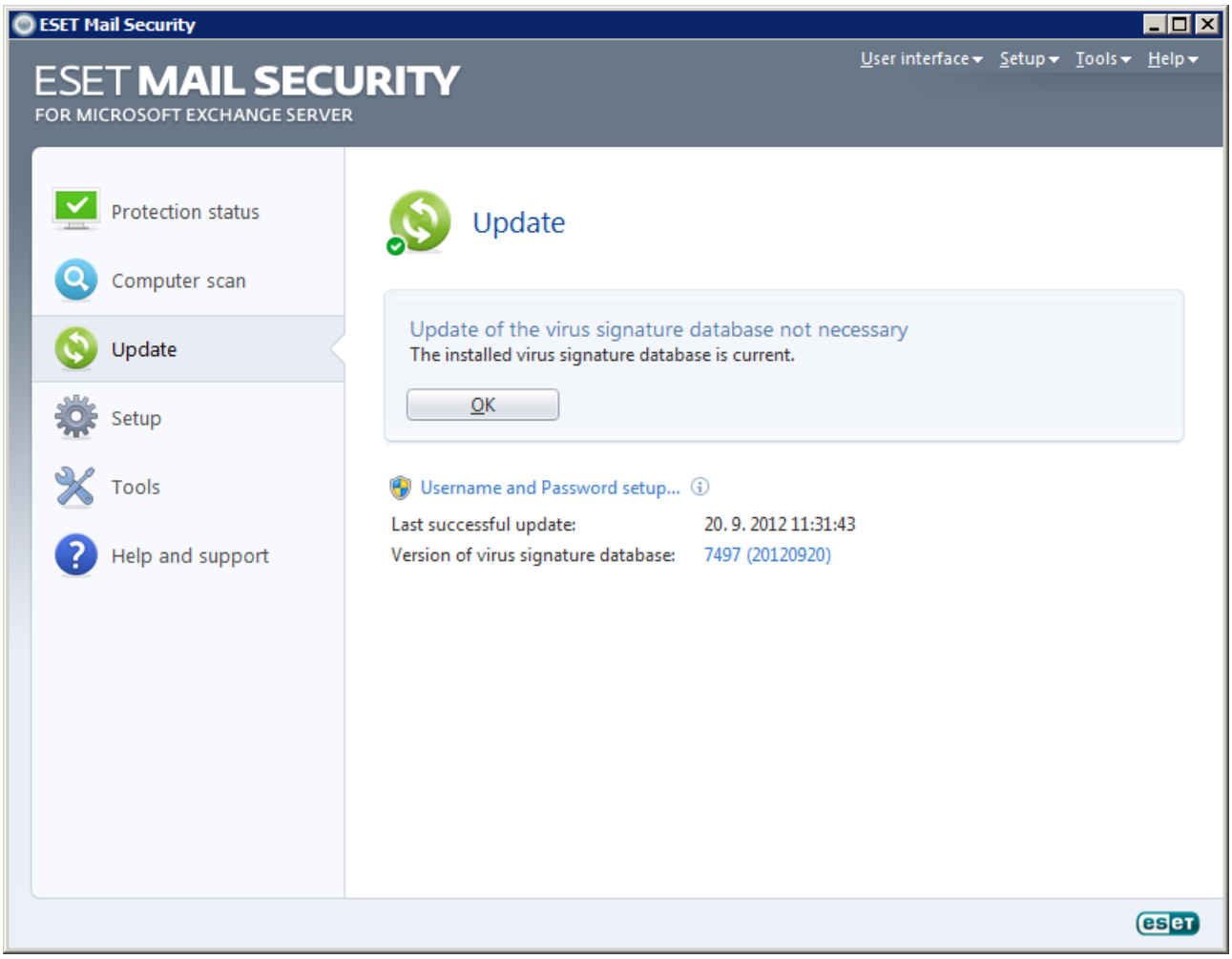
4.2 Updating the program

Regular updating of ESET Mail Security is the basic premise for obtaining the maximum level of security. The Update module ensures that the program is always up to date in two ways – by updating the virus signature database and by updating system components.

By clicking **Update** from the main menu, you can find the current update status, including the date and time of the last successful update and if an update is needed. The primary window also contains the virus signature database version. This numeric indicator is an active link to ESET's website, listing all signatures added within the given update.

In addition, the option to manually begin the update process – **Update virus signature database** – is available, as well as basic update setup options such as the username and password to access ESET's update servers.

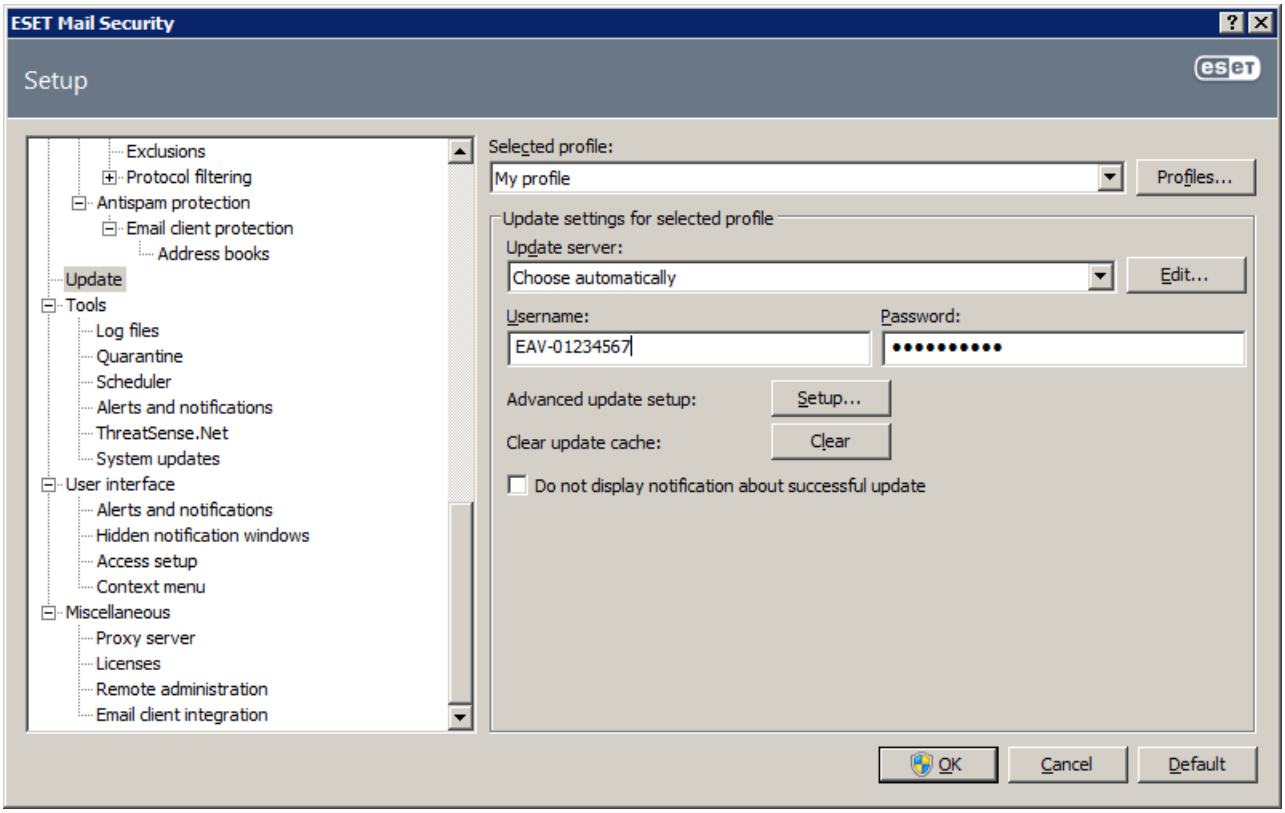
Use the **Product activation** link to open a registration form that will activate your ESET security product and send you an email with your authentication data (username and password).



NOTE: The username and password are provided by ESET after purchasing ESET Mail Security.

4.2.1 Update setup

The update setup section specifies update source information such as the update servers and authentication data for these servers. By default, the **Update server** drop-down menu is set to **Choose automatically** to ensure that update files will automatically download from the ESET server with the least network traffic. The update setup options are available from the Advanced Setup tree (F5 key), under **Update**.

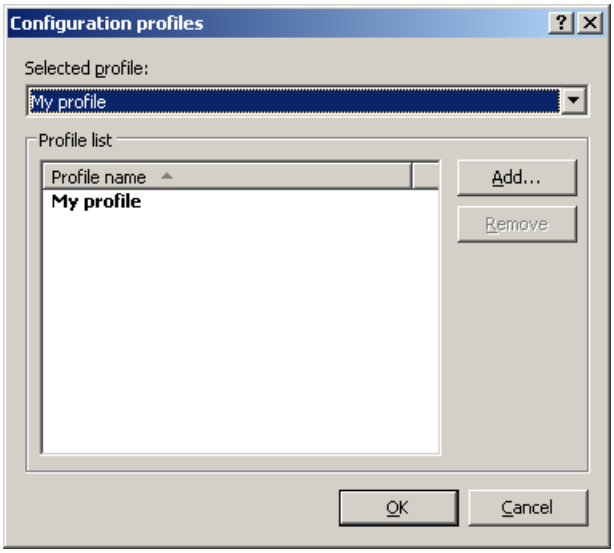


The list of available update servers is accessible via the **Update server** drop-down menu. To add a new update server, click **Edit...** in the **Update settings for selected profile** section and then click the **Add** button. Authentication for update servers is based on the **Username** and **Password** generated and sent to you after purchase.

4.2.1.1 Update profiles

Update profiles can be created for various update configurations and tasks. Creating update profiles is especially useful for mobile users, who can create an alternative profile for Internet connection properties that regularly change.

The **Selected profile** drop-down menu displays the currently selected profile, set to **My profile** by default. To create a new profile, click the **Profiles...** button and then click the **Add...** button and enter your own **Profile name**. When creating a new profile, you can copy settings from an existing one by selecting it from the **Copy settings from profile** drop-down menu.



In the profile setup window, you can specify the update server from a list of available servers or add a new server. The list of existing update servers is accessible via the **Update server**: drop-down menu. To add a new update server, click **Edit...** in the **Update settings for selected profile** section and then click the **Add** button.

4.2.1.2 Advanced update setup

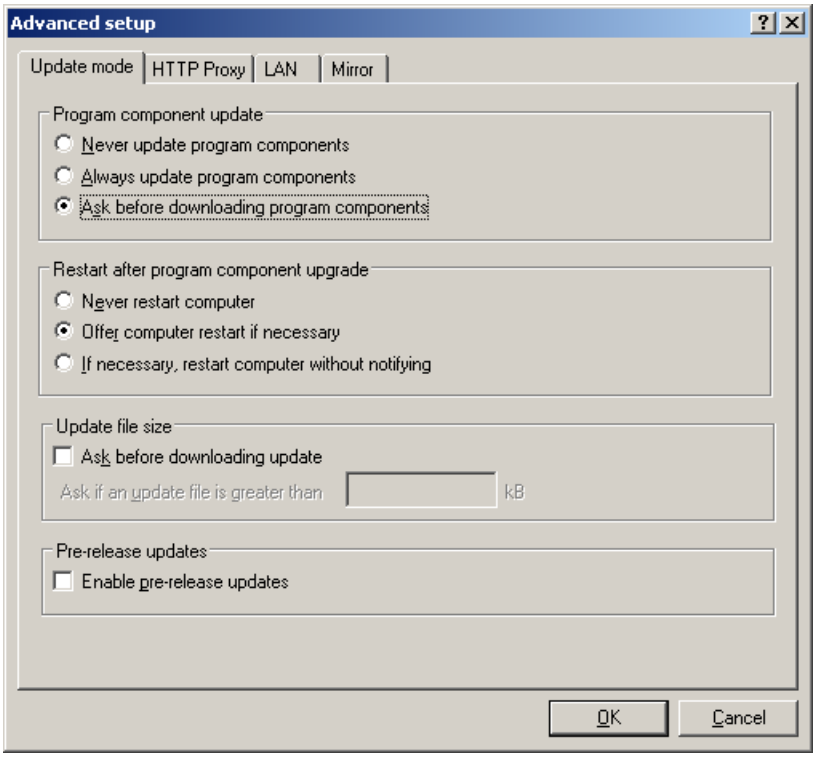
To view the Advanced update setup, click the **Setup...** button. Advanced update setup options include configuration of **Update mode**, **HTTP Proxy**, **LAN** and **Mirror**.

4.2.1.2.1 Update mode

The **Update mode** tab contains options related to the program component update.

In the **Program component update** section, three options are available:

- **Never update program components**: New program component updates will not be downloaded.
- **Always update program components**: New program component updates will occur automatically.
- **Ask before downloading program components**: The default option. You will be prompted to confirm or refuse program component updates when they are available.



After a program component update, it may be necessary to restart your computer to provide full functionality of all modules. The **Restart after program component upgrade** section allows you to select one of the following options:

- **Never restart computer**
- **Offer computer restart if necessary**
- **If necessary**, **restart computer without notifying**

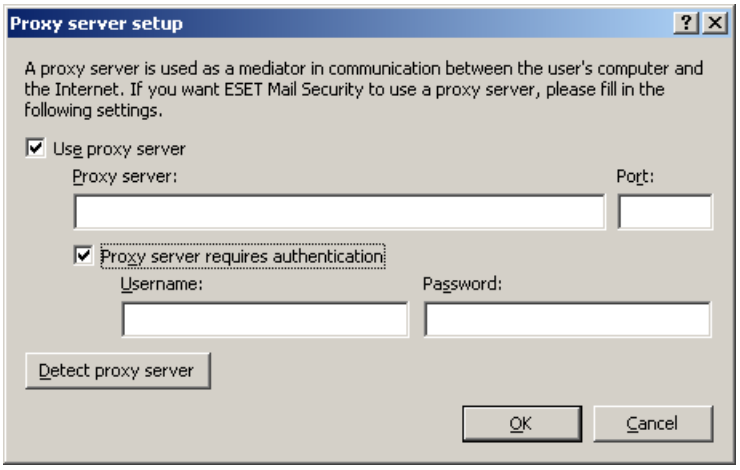
The default option is **Offer computer restart if necessary**. Selection of the most appropriate option depends on the workstation where the settings will be applied. Please be aware that there are differences between workstations and servers – e.g., restarting the server automatically after a program upgrade could cause serious damage.

4.2.1.2.2 Proxy server

In ESET Mail Security, proxy server setup is available in two different sections within the Advanced Setup tree.

First, proxy server settings can be configured under **Miscellaneous** > **Proxy server**. Specifying the proxy server at this level defines global proxy server settings for all of ESET Mail Security. Parameters here will be used by all modules requiring connection to the Internet.

To specify proxy server settings for this level, select the **Use proxy server** checkbox and then enter the address of the proxy server into the **Proxy server**: field, along with the **Port** number of the proxy server.


Proxy server setup
A proxy server is used as a mediator in communication between the user's computer and the Internet. If you want ESET Mail Security to use a proxy server, please fill in the following settings.
Use proxy server
Proxy server:
Port:
Proxy server requires authentication
Username:
Password:
Detect proxy server
OK
Cancel

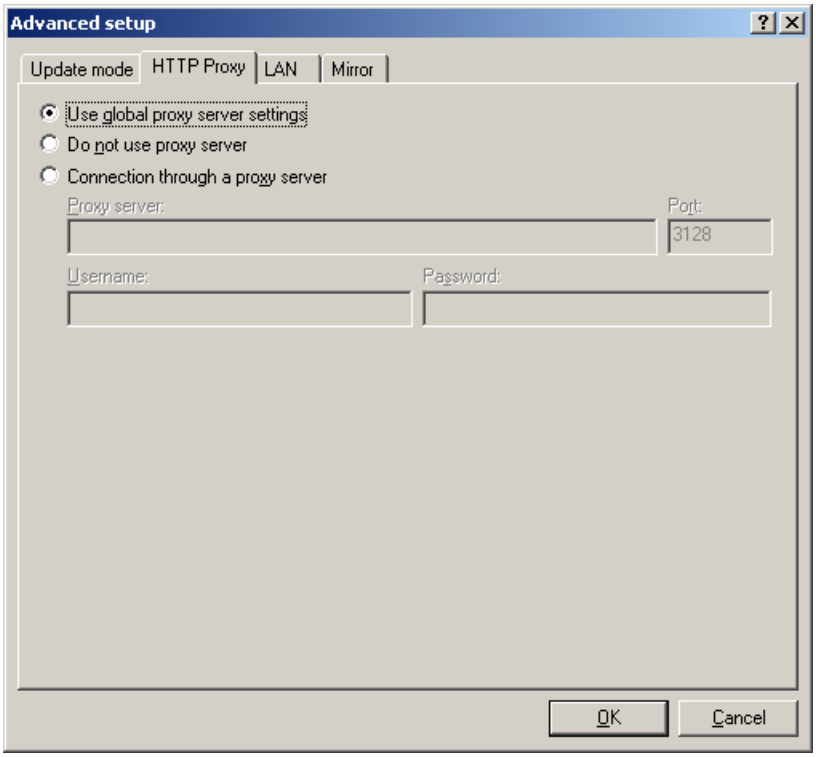
If communication with the proxy server requires authentication, select the **Proxy server requires authentication** checkbox and enter a valid **Username** and **Password** into the respective fields. Click the **Detect proxy server** button to automatically detect and insert proxy server settings. The parameters specified in Internet Explorer will be copied.

NOTE: This feature does not retrieve authentication data (username and password), it must be supplied by you.

Proxy server settings can also be established within Advanced update setup. This setting applies for the given update profile. You can access the proxy server setup options for a given update profile by clicking on the **HTTP Proxy** tab in **Advanced update setup**. You will have one of the three following options:

- **Use global proxy server settings**
- **Do not use proxy server**
- **Connection through a proxy server** (connection defined by the connection properties)

Selecting the **Use global proxy server settings** option will use the proxy server configuration options already specified within the **Miscellaneous** > **Proxy server** branch of the Advanced Setup tree (as described at the top of this article).



Select the **Do not use proxy server** option to specify that no proxy server will be used to update ESET Mail Security.

The **Connection through a proxy server** option should be selected if a proxy server should be used to update ESET Mail Security and is different from the proxy server specified in the global settings (**Miscellaneous** > **Proxy server**). If so, the settings should be specified here: **Proxy server** address, communication **Port**, plus **Username** and **Password** for the proxy server, if required.

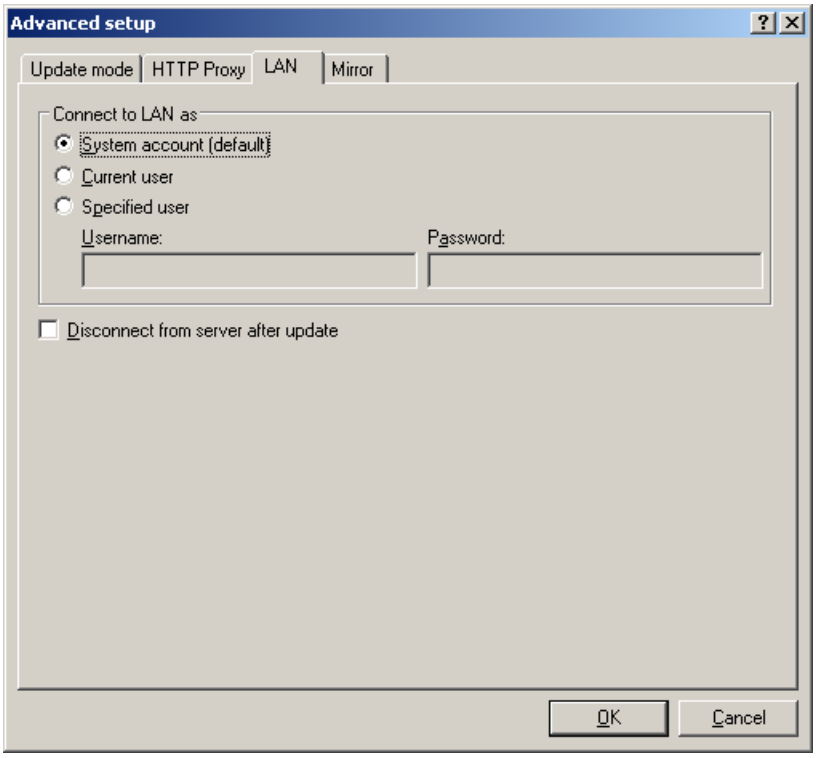
This option should also be selected if the proxy server settings were not set globally, but ESET Mail Security will connect to a proxy server for updates.

The default setting for the proxy server is **Use global proxy server settings**.

4.2.1.2.3 Connecting to the LAN

When updating from a local server with an NT-based operating system, authentication for each network connection is required by default. In most cases, a local system account does not have sufficient rights to access the Mirror folder (the Mirror folder contains copies of update files). If this is the case, enter the username and password in the update setup section, or specify an existing account under which the program will access the update server (Mirror).

To configure such an account, click the **LAN** tab. The **Connect to LAN as** section offers the **System account** (**default**), **Current user**, and **Specified user** options.



Select the **System account** (**default**) option to use the system account for authentication. Normally, no authentication process takes place if there is no authentication data supplied in the main update setup section.

To ensure that the program authenticates using a currently logged-in user account, select **Current user**. The drawback of this solution is that the program is not able to connect to the update server if no user is currently logged in.

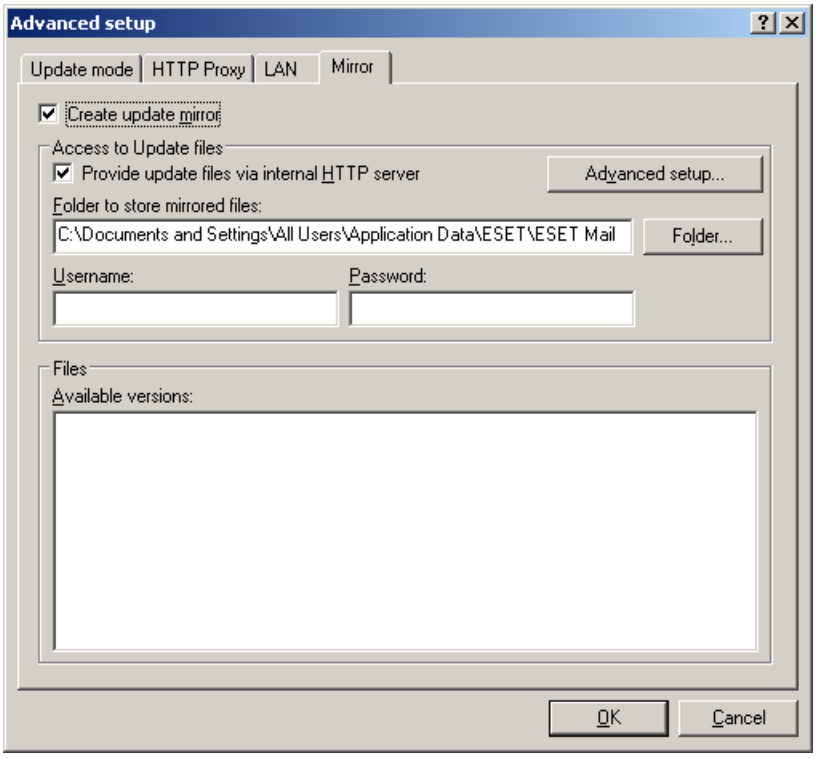
Select **Specified user** if you want the program to use a specific user account for authentication.

Warning: When either **Current user** or **Specified user** is selected, an error may occur when changing the identity of the program to the desired user. We recommend inserting the LAN authentication data in the main update setup section. In this update setup section, the authentication data should be entered as follows: domain_name\user (if it is a workgroup, enter workgroup_name\name) and password. When updating from the HTTP version of the local server, no authentication is required.

4.2.1.2.4 Creating update copies - Mirror

ESET Mail Security allows you to create copies of update files which can be used to update other workstations located in the network. Updating client workstations from a Mirror optimizes network load balance and saves Internet connection bandwidth.

Configuration options for the local Mirror server are accessible (after adding a valid license key in the license manager, located in the ESET Mail Security Advanced Setup section) in the **Advanced update setup**: section. To access this section, press F5 and click **Update** in the Advanced Setup tree, then click the **Setup...** button next to **Advanced update setup**: and select the **Mirror** tab).



The first step in configuring the Mirror is to select the Create update mirror option. Selecting this option activates other Mirror configuration options such as the way update files will be accessed and the update path to the mirrored files.

The methods of Mirror activation are described in detail in section Updating from the Mirror 86. For now, note that there are two basic methods for accessing the Mirror – the folder with update files can be presented as a shared network folder or as an HTTP server.

The folder dedicated to storing update files for the Mirror is defined in the **Folder to store mirrored files** section. Click **Folder...** to browse for a folder on the local computer or shared network folder. If authorization for the specified folder is required, authentication data must be supplied in the **Username** and **Password** fields. The username and password should be entered in the format *Domain/ User* or *Workgroup/User*. Please remember to supply the corresponding passwords.

When configuring the Mirror, you can also specify the language versions for which you want to download update copies. Language version setup is accessible in the section **Files - Available versions**:.

NOTE: It is not possible for Antispam database to be updated from the mirror. To read more information on how to allow for correct Antispam database updates, click here 35.

4.2.1.2.4.1 Updating from the Mirror

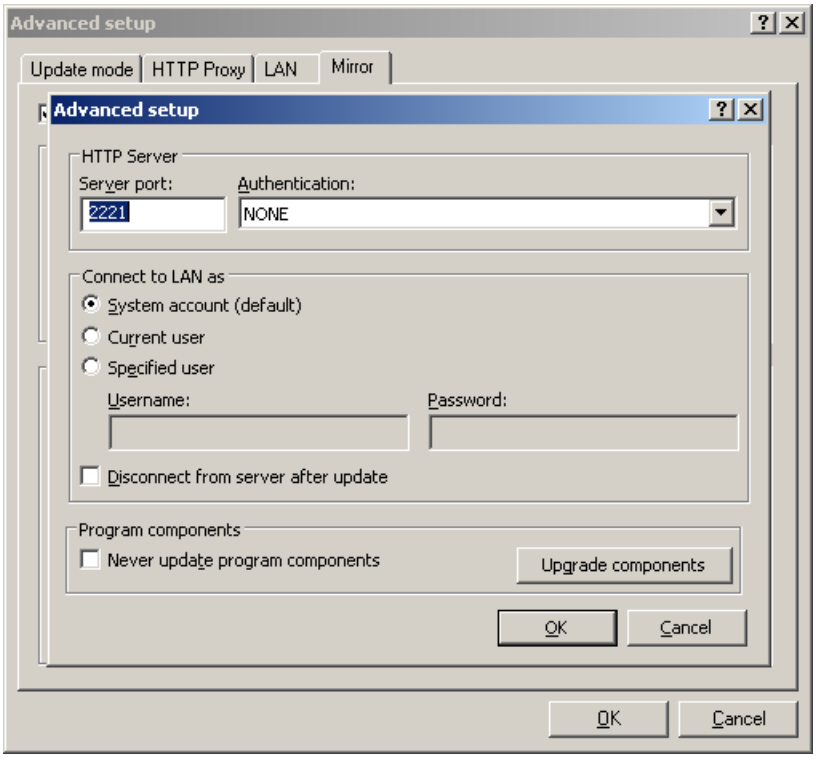
There are two basic methods of configuring the Mirror – the folder with update files can be presented as a shared network folder or as an HTTP server.

Accessing the Mirror using an internal HTTP server

This configuration is the default, specified in the predefined program configuration. In order to allow access to the Mirror using the HTTP server, navigate to **Advance update setup** (the **Mirror** tab) and select the **Create update mirror** option.

In the **Advanced setup** section of the **Mirror** tab you can specify the **Server Port** where the HTTP server will listen as well as the type of **Authentication** used by the HTTP server. By default, the Server port is set to **2221**. The **Authentication** option defines the method of authentication used for accessing the update files. The following options are available: **NONE**, **Basic**, and **NTLM**. Select **Basic** to use the base64 encoding with basic username and password authentication. The **NTLM** option provides encoding using a safe encoding method. For authentication, the user created on the workstation sharing the update files is used. The default setting is **NONE**, which grants access to the update files with no need for authentication.

Warning: If you want to allow access to the update files via the HTTP server, the Mirror folder must be located on the same computer as the ESET Mail Security instance creating it.



After configuration of the Mirror is complete, go to the workstations and add a new update server in the format **http://IP_address_of_your_server:2221**. To do this, follow the steps below:

- Open ESET Mail Security **Advanced Setup** and click the **Update** branch.
- Click **Edit...** to the right of the **Update server** drop-down menu and add a new server using the following format: http://IP_address_of_your_server:2221.
- Select this newly-added server from the list of update servers.

Accessing the Mirror via system shares

First, a shared folder should be created on a local or a network device. When creating the folder for the Mirror, you must provide "write" access for the user who will save update files to the folder and "read" access for all users who will update ESET Mail Security from the Mirror folder.

Next, configure access to the Mirror in the **Advanced update setup** section (**Mirror** tab) by disabling the **Provide update files via internal HTTP server** option. This option is enabled by default in the program install package.

If the shared folder is located on another computer in the network, you must specify authentication data to access

the other computer. To specify authentication data, open ESET Mail Security Advanced Setup (F5) and click the **Update** branch. Click the **Setup...** button and then click the **LAN** tab. This setting is the same as for updating, as described in section Connecting to LAN 84.

After the Mirror configuration is complete, proceed to the workstations and set \\UNC\PATH as the update server. This operation can be completed using the following steps:

- Open ESET Mail Security Advanced Setup and click **Update**
- Click **Edit...** next to the Update server and add a new server using the *UNC**PATH format*.
- Select this newly-added server from the list of update servers

NOTE: For proper functioning, the path to the Mirror folder must be specified as a UNC path. Updates from mapped drives may not work.

4.2.1.2.4.2 Troubleshooting Mirror update problems

In most cases, problems during an update from a Mirror server are caused by one or more of the following: incorrect specification of the Mirror folder options, incorrect authentication data to the Mirror folder, incorrect configuration on local workstations attempting to download update files from the Mirror, or by a combination of the reasons above. Below is an overview of the most frequent problems which may occur during an update from the Mirror:

ESET Mail Security **reports an error connecting to Mirror server** – Likely caused by incorrect specification of the update server (network path to the Mirror folder) from which local workstations download updates. To verify the folder, click the Windows **Start** menu, click **Run**, insert the folder name and click **OK**. The contents of the folder should be displayed.

ESET Mail Security **requires a username and password** – Likely caused by incorrect authentication data (username and password) in the update section. The username and password are used to grant access to the update server, from which the program will update itself. Make sure that the authentication data is correct and entered in the correct format. For example, *Domain/Username*, or *Workgroup/ Username*, plus the corresponding Passwords. If the Mirror server is accessible to "Everyone", please be aware that this does not mean that any user is granted access. "Everyone" does not mean any unauthorized user, it just means that the folder is accessible for all domain users. As a result, if the folder is accessible to "Everyone", a domain username and password will still need to be entered in the update setup section.

ESET Mail Security **reports an error connecting to the Mirror server** – Communication on the port defined for accessing the HTTP version of the Mirror is blocked.

4.2.2 How to create update tasks

Updates can be triggered manually by clicking **Update virus signature database** in the primary window displayed after clicking Update from the main menu.

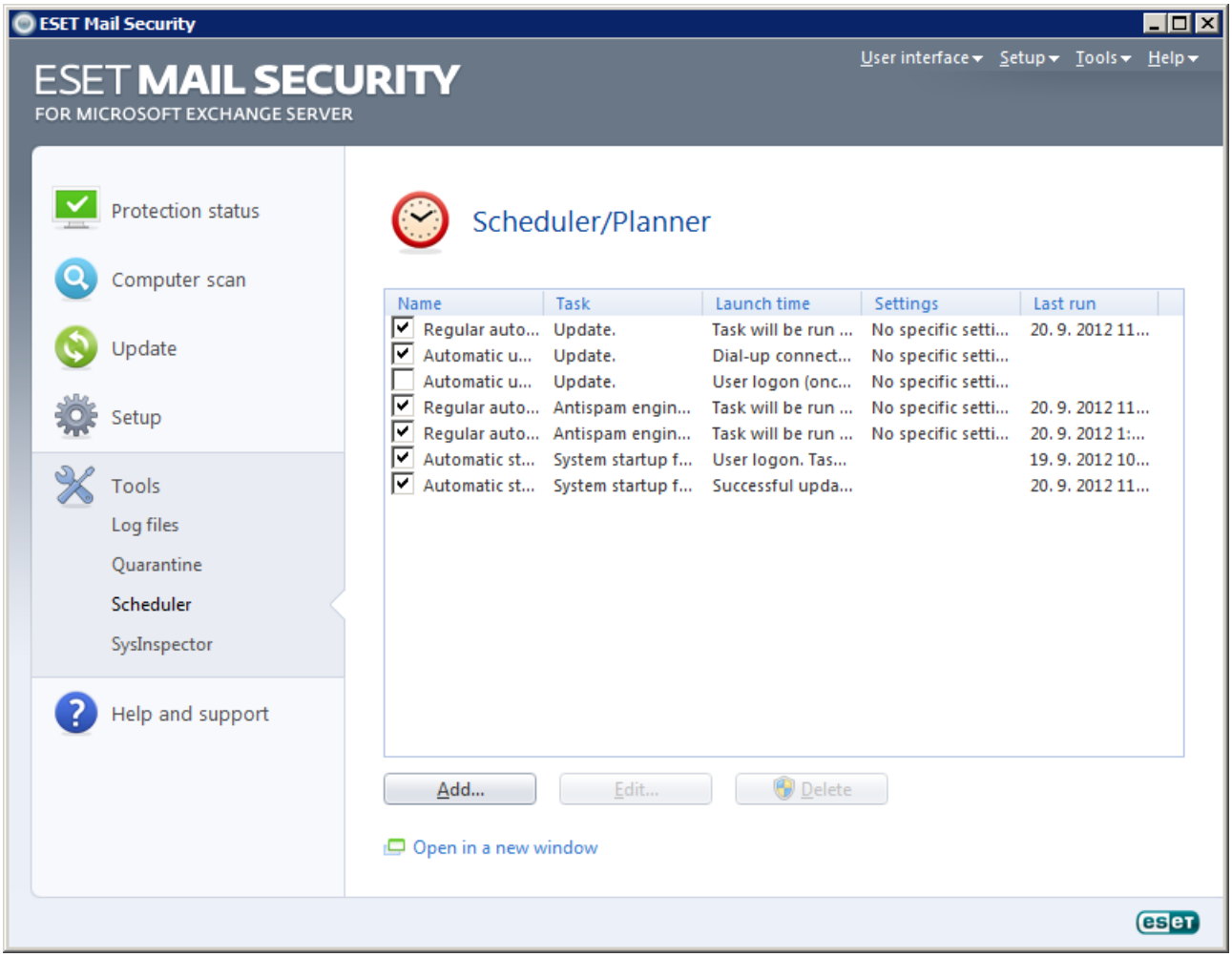
Updates can also be run as scheduled tasks. To configure a scheduled task, click **Tools** > **Scheduler**. By default, the following tasks are activated in ESET Mail Security:

- **Regular automatic update**
- **Automatic update after dial-up connection**
- **Automatic update after user logon**

Each update task can be modified to meet your needs. In addition to the default update tasks, you can create new update tasks with a user-defined configuration. For more details about creating and configuring update tasks, see section Scheduler 88.

4.3 Scheduler

Scheduler is available if Advanced mode in ESET Mail Security is activated. **Scheduler** can be found in the ESET Mail Security main menu under **Tools**. Scheduler contains a list of all scheduled tasks and configuration properties such as the predefined date, time, and scanning profile used.



By default, the following scheduled tasks are displayed in **Scheduler**:

- **Regular automatic update**
- **Automatic update after dial-up connection**
- **Automatic update after user logon**
- **Automatic startup file check (after user logon)**
- **Automatic startup file check (after successful update of the virus signature database)**

To edit the configuration of an existing scheduled task (both default and user-defined), right-click the task and click **Edit...** or select the desired task you wish to modify and click the **Edit...** button.

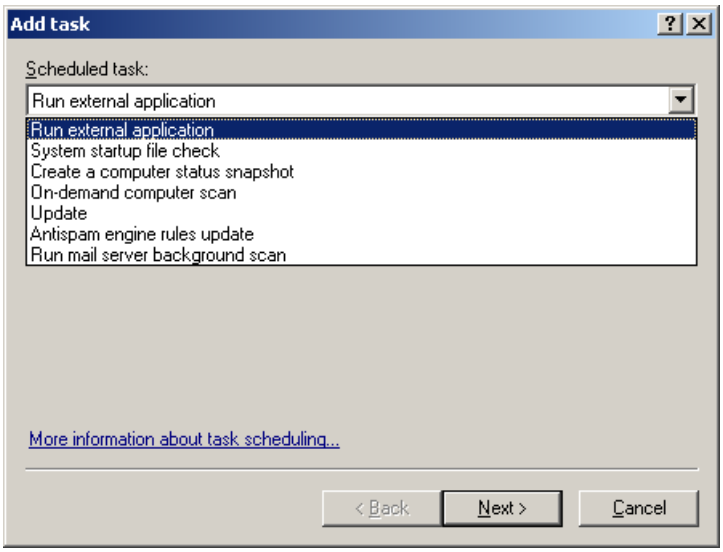
4.3.1 Purpose of scheduling tasks

Scheduler manages and launches scheduled tasks with predefined configuration and properties. The configuration and properties contain information such as the date and time as well as specified profiles to be used during execution of the task.

4.3.2 Creating new tasks

To create a new task in Scheduler, click the **Add...** button or right-click and select **Add...** from the context menu. Five types of scheduled tasks are available:

- **Run external application**
- **System startup file check**
- **Create a computer status snapshot**
- **On-demand computer scan**
- **Update**



Since **Update** is one of the most frequently used scheduled tasks, we will explain how to add a new update task.

From the **Scheduled task**: drop-down menu, select **Update**. Click **Next** and enter the name of the task into the **Task name**: field. Select the frequency of the task. The following options are available: **Once**, **Repeatedly**, **Daily**, **Weekly** and **Event triggered**. Based on the frequency selected, you will be prompted with different update parameters. Next, define what action to take if the task cannot be performed or completed at the scheduled time. The following three options are available:

- **Wait until the next scheduled time**
- **Run task as soon as possible**
- **Run task immediately if the time since its last execution exceeds specified interval** (the interval can be defined using the Task interval scroll box)

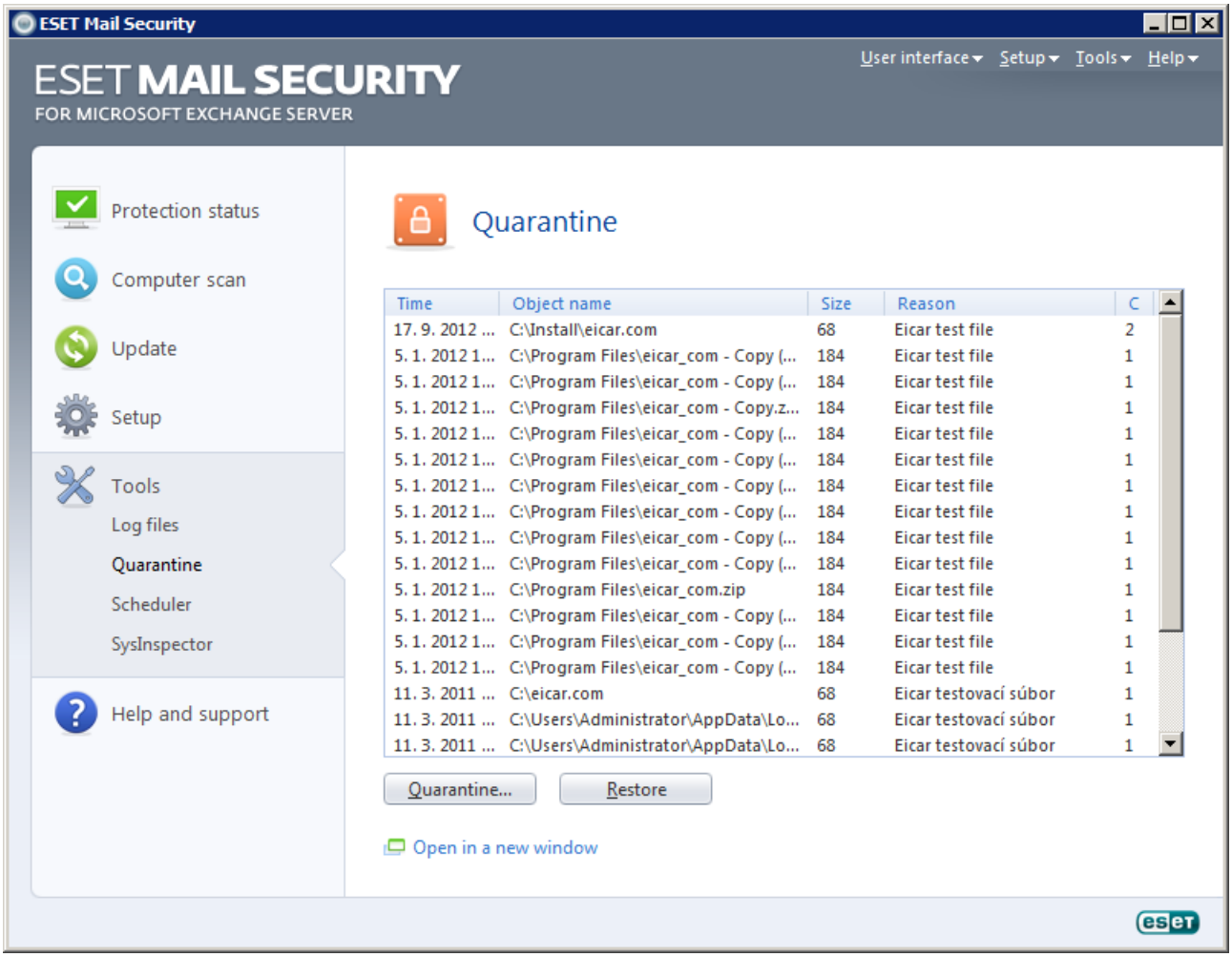
In the next step, a summary window with information about the current scheduled task is displayed; the option **Run task with specific parameters** should be automatically enabled. Click the **Finish** button.

A dialog window will appear, allowing you to select profiles to be used for the scheduled task. Here you can specify a primary and alternative profile, which is used in case the task cannot be completed using the primary profile. Confirm by clicking **OK** in the **Update profiles** window. The new scheduled task will be added to the list of currently scheduled tasks.

4.4 Quarantine

The main task of quarantine is to safely store infected files. Files should be quarantined if they cannot be cleaned, if it is not safe or advisable to delete them, or if they are being falsely detected by ESET Mail Security.

You can choose to quarantine any file. This is advisable if a file behaves suspiciously but is not detected by the antivirus scanner. Quarantined files can be submitted for analysis to ESET's Threat Lab.


ESET Mail Security
ESET MAIL SECURITY
FOR MICROSOFT EXCHANGE SERVER
User interface
Setup
Tools
Help
Protection status
Computer scan
Update
Setup
Tools
Log files
Quarantine
Scheduler
SysInspector
Help and support
Quarantine
Time
Object name
Size
Reason
C
17. 9. 2012 ... C:\Install\eicar.com 68 Eicar test file 2
5. 1. 2012 1... C:\Program Files\eicar_com - Copy (... 184 Eicar test file 1
5. 1. 2012 1... C:\Program Files\eicar_com - Copy (... 184 Eicar test file 1
5. 1. 2012 1... C:\Program Files\eicar_com - Copy.z... 184 Eicar test file 1
5. 1. 2012 1... C:\Program Files\eicar_com - Copy (... 184 Eicar test file 1
5. 1. 2012 1... C:\Program Files\eicar_com - Copy (... 184 Eicar test file 1
5. 1. 2012 1... C:\Program Files\eicar_com - Copy (... 184 Eicar test file 1
5. 1. 2012 1... C:\Program Files\eicar_com - Copy (... 184 Eicar test file 1
5. 1. 2012 1... C:\Program Files\eicar_com - Copy (... 184 Eicar test file 1
5. 1. 2012 1... C:\Program Files\eicar_com - Copy (... 184 Eicar test file 1
5. 1. 2012 1... C:\Program Files\eicar_com.zip 184 Eicar test file 1
5. 1. 2012 1... C:\Program Files\eicar_com - Copy (... 184 Eicar test file 1
5. 1. 2012 1... C:\Program Files\eicar_com - Copy (... 184 Eicar test file 1
5. 1. 2012 1... C:\Program Files\eicar_com - Copy (... 184 Eicar test file 1
11. 3. 2011 ... C:\eicar.com 68 Eicar testovací súbor 1
11. 3. 2011 ... C:\Users\Administrator\AppData\Lo... 68 Eicar testovací súbor 1
11. 3. 2011 ... C:\Users\Administrator\AppData\Lo... 68 Eicar testovací súbor 1
Quarantine...
Restore
Open in a new window
eset

Files stored in the quarantine folder can be viewed in a table which displays the date and time of quarantine, the path to the original location of the infected file, its size in bytes, reason (**added by user...**), and number of threats (e.g., if it is an archive containing multiple infiltrations).

4.4.1 Quarantining files

ESET Mail Security automatically quarantines deleted files (if you have not cancelled this option in the alert window). If desired, you can quarantine any suspicious file manually by clicking the **Quarantine...** button. If this is the case, the original file is not removed from its original location. The context menu can also be used for this purpose – right-click in the **Quarantine** window and select **Add...**

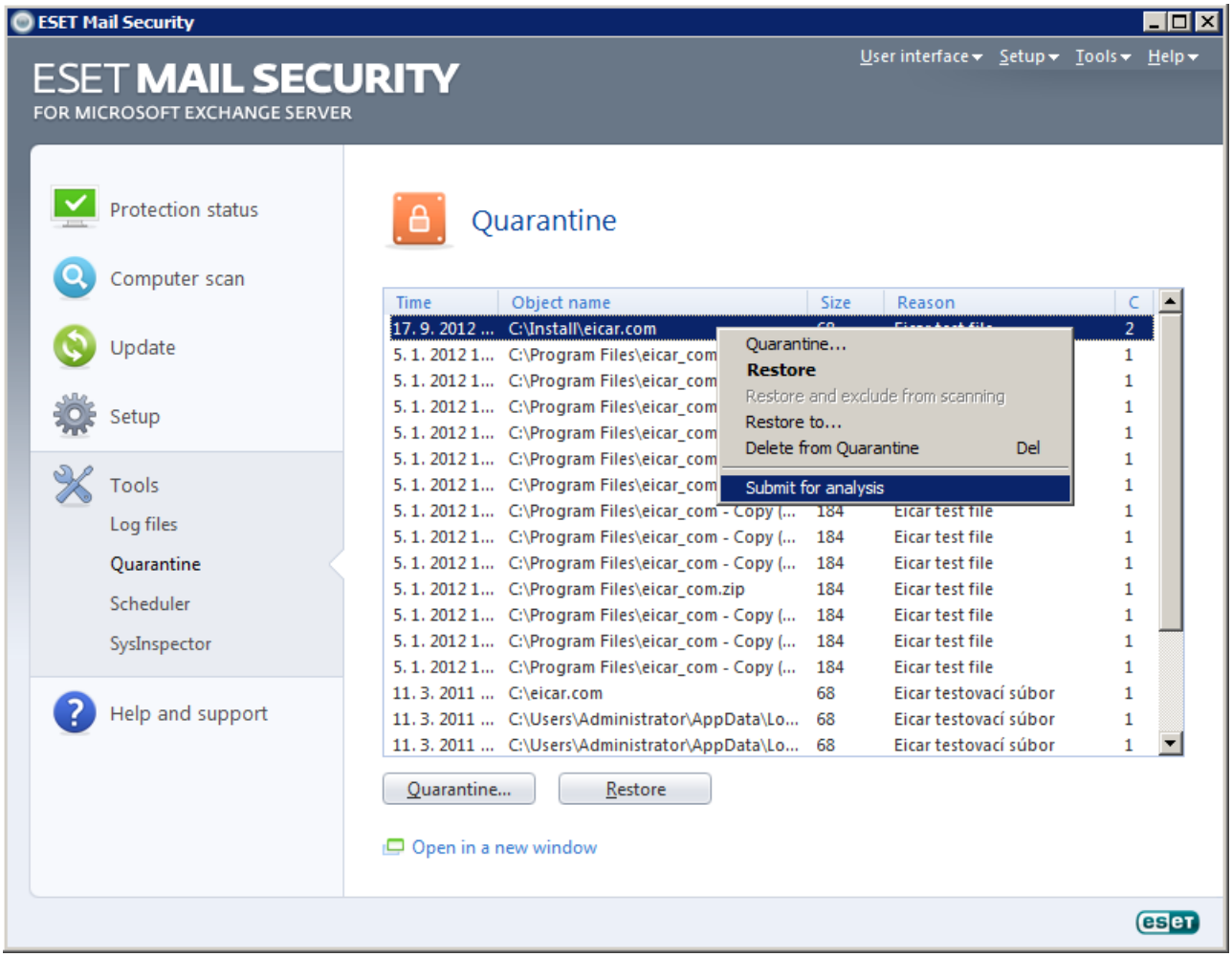
4.4.2 Restoring from Quarantine

Quarantined files can be restored to their original location. Use the **Restore** feature for this purpose. **Restore** is available from the context menu by right-clicking on the given file in the Quarantine window. The context menu also offers the **Restore to** option, which allows you to restore a file to a location other than the one from which it was deleted.

NOTE: If the program quarantined a harmless file by mistake, please exclude the file from scanning after restoring and send the file to ESET Customer Care.

4.4.3 Submitting file from Quarantine

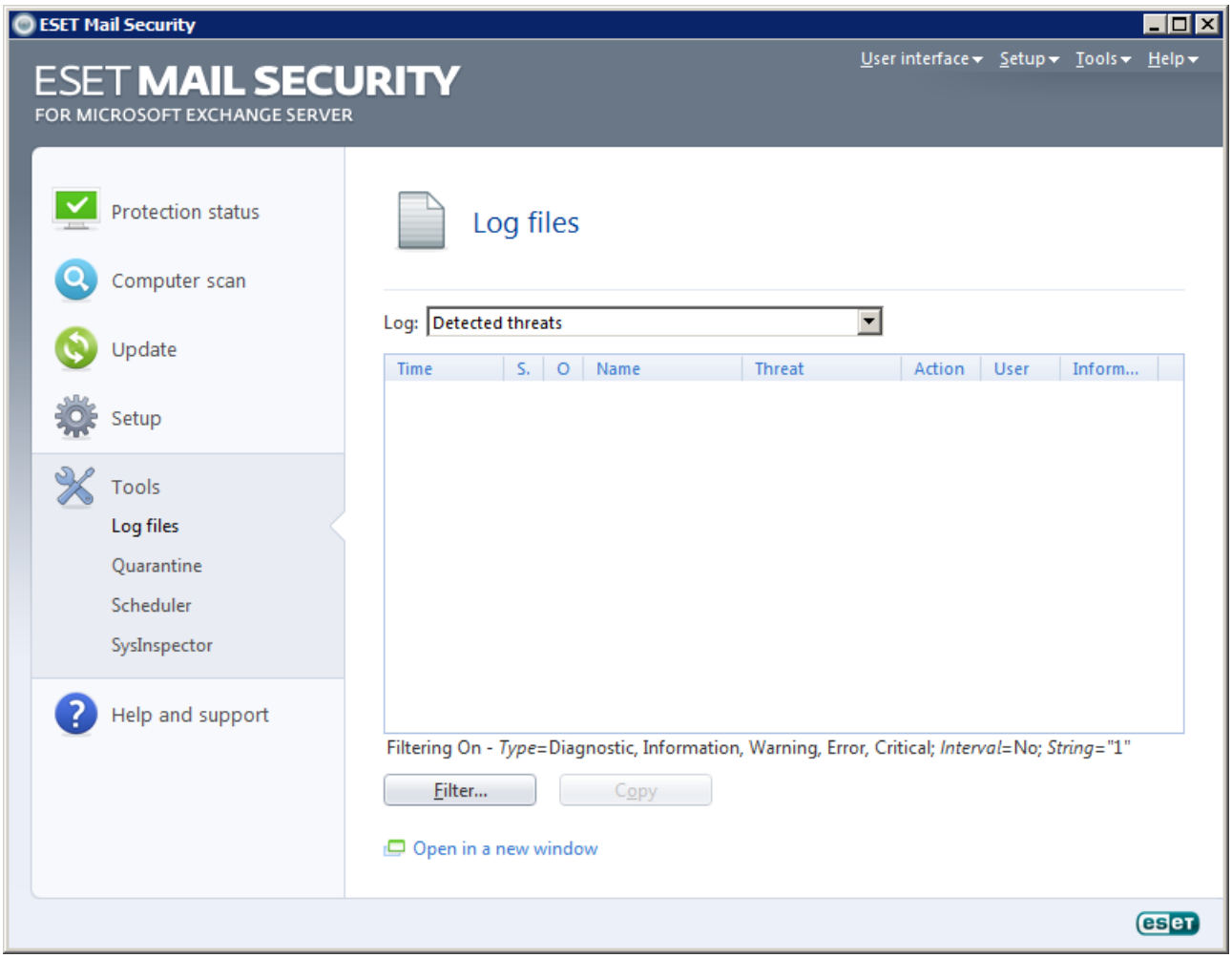
If you have quarantined a suspicious file that was not detected by the program, or if a file was incorrectly evaluated as infected (e.g., by heuristic analysis of the code) and subsequently quarantined, please send the file to ESET's Threat Lab. To submit a file from quarantine, right-click the file and select **Submit for analysis** from the context menu.


ESET Mail Security
ESET MAIL SECURITY
FOR MICROSOFT EXCHANGE SERVER
User interface
Setup
Tools
Help
Protection status
Computer scan
Update
Setup
Tools
Log files
Quarantine
Scheduler
SysInspector
Help and support
Quarantine
Time
Object name
Size
Reason
C
17. 9. 2012 ... C:\Install\eicar.com 2
5. 1. 2012 1... C:\Program Files\eicar_com 1
5. 1. 2012 1... C:\Program Files\eicar_com 1
5. 1. 2012 1... C:\Program Files\eicar_com 1
5. 1. 2012 1... C:\Program Files\eicar_com 1
5. 1. 2012 1... C:\Program Files\eicar_com 1
5. 1. 2012 1... C:\Program Files\eicar_com 1
5. 1. 2012 1... C:\Program Files\eicar_com - Copy (... 184 Eicar test file 1
5. 1. 2012 1... C:\Program Files\eicar_com - Copy (... 184 Eicar test file 1
5. 1. 2012 1... C:\Program Files\eicar_com - Copy (... 184 Eicar test file 1
5. 1. 2012 1... C:\Program Files\eicar_com.zip 184 Eicar test file 1
5. 1. 2012 1... C:\Program Files\eicar_com - Copy (... 184 Eicar test file 1
5. 1. 2012 1... C:\Program Files\eicar_com - Copy (... 184 Eicar test file 1
5. 1. 2012 1... C:\Program Files\eicar_com - Copy (... 184 Eicar test file 1
11. 3. 2011 ... C:\eicar.com 68 Eicar testovací súbor 1
11. 3. 2011 ... C:\Users\Administrator\AppData\Lo... 68 Eicar testovací súbor 1
11. 3. 2011 ... C:\Users\Administrator\AppData\Lo... 68 Eicar testovací súbor 1
Quarantine...
Restore and exclude from scanning
Restore to...
Delete from Quarantine Del
Submit for analysis
Quarantine...
Restore
Open in a new window
eset

4.5 Log files

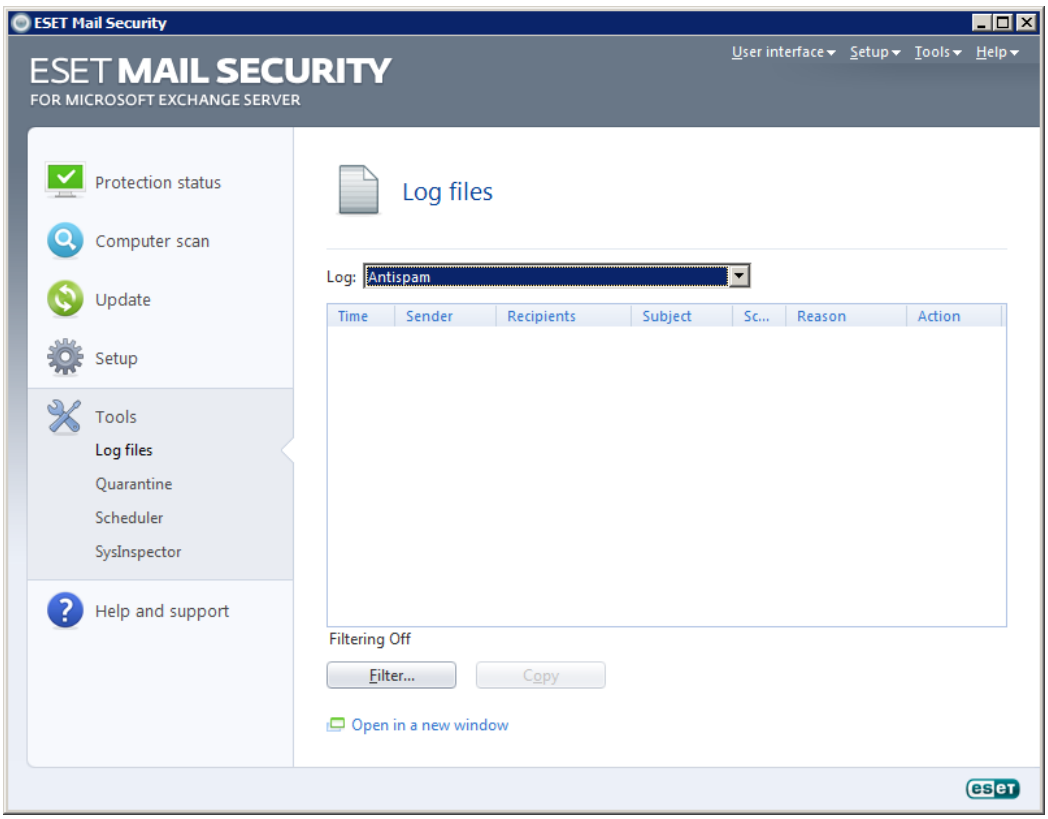
Logs store information about important events: detected infiltrations, logs from the on-demand scanner, logs from the resident scanners and system information.

Antispam and greylisting protection logs (found under other logs under **Tools** > **Log files**) contain detailed information about messages that were subject to scanning and the consequent actions performed on those messages. Logs can be very useful when looking for undelivered email, trying to figure why a message was marked as spam, etc.



Antispam

All messages categorized by the ESET Mail Security as spam or probable spam are recorded here.



Columns description:

Time – time of entry into the antispam log

Sender – sender's address

Recipient – recipient's address

Subject – message subject

Score – spam score assigned to the message (in range from 0 to 100)

Reason – is an indicator which caused the message to be classified as spam. The displayed indicator is the strongest. If you want to see the other indicators, double-click the entry. The **Reason** window will open containing the remaining indicators sorted descending by strength.

URL Spammy Reputation	URL addresses in messages can often be an indication of spam.
HTML Formatting (Fonts, colors, etc)	Formatting of elements in the HTML part of the message shows signs characteristic for spam (font type and size, it's color etc.)
Spam Tricks: Obfuscation	Words typical for spam tend to be masked by using other characters. A typical example is the word "Viagra", which is often written as "V1agra" to evade anstispam detection.
HTML Image Type spam	Spam messages often take the form of pictures as another evasive strategy applied against antispam detection methods. Such pictures usually contain interactive links to web pages.
URL formatting hosting service domain	URL address contains the hosting service domain.
Spammy keyword ...	Message contains words typical for spam.
Email header inconsistency	Information in the header is altered to pose as a source other than the original sender.
Virus	Message contains a suspicious attachment.

Phish	Message contains text that is typical to phishing messages.
Replica	Message contains text that is typical for a category of spam oriented at offering replicas.
Generic spam indicator	Message containing words/characters that is typical for spam, as e.g. "Dear friend", "hello winner", "!!!" etc.
Ham indicator	This is an indicator that has the opposite function as the other listed indicators. It analyzes elements characteristic for regular solicited mail. It lowers the overall spam score.
Non-specific spam indicator	Message contains other spam elements, such as base64 coding.
Custom spam phrases	Other typical spam phrases.
URL is blacklisted	URL in the message is on a blacklist.
IP %s is on RBL	IP address ... is on a RBL list.
URL %s is on DNSBL	URL address ... is on a DNSBL list.
URL %s is on RBL or the server is not entitled to send mail	URL address ... is on a RBL list, or the server does not have the required privileges to send email messages. Addresses which were part of the email's route are verified against the RBL list. The last address is tested regarding its connectivity rights to public mail servers. If it's impossible to detect valid connectivity rights, the address is on the LBL list. Messages marked as spam, because of an LBL indicator have the following text stated in their **Reason** field: "server is not entitled to send mail".

Action – action performed on the message. Possible actions:

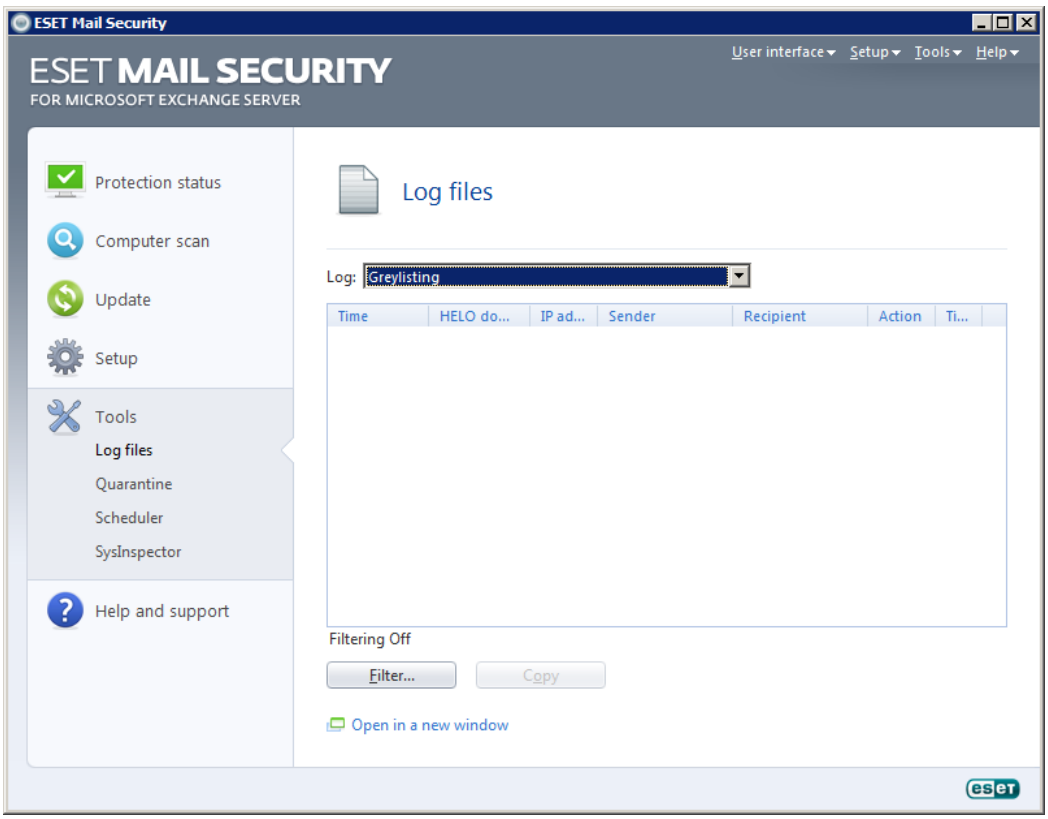
Retained	No action has been performed on the message.
Quarantined	Message was moved into quarantine.
Cleaned and quarantined	The virus had been removed from the message and the message was quarantined.
Rejected	Message was denied and the SMTP reject answer 19 sent to the sender.
Deleted	Message was deleted using silent drop 19.

Received – time the message was received by the server.

NOTE: If mails are received via an email server, the times in the **Time** and **Received** fields are practically identical.

Greylisting

All messages that have been evaluated using the greylisting method are recorded in this log.



Columns description:

Time – time of entry into the antispam log

HELO Domain – domain name used by the sending server to identify itself towards the receiving server

IP address – sender's IP address

Sender – sender's address

Recipient – recipient's address

Action – may contain the following statuses:

Rejected	The incoming message was denied using the basic precept of greylisting (first delivery attempt)
Rejected (not verified)	The incoming message was redelivered by the sending server, but the time limit to deny the connection has not elapsed yet (**Time limit for the initial connection denial**).
Verified	The incoming message was redelivered several times by the sending server, the **Time limit for the initial connection denial** has elapsed and the message was successfully verified and delivered. See also Transport agent 36.

Time remaining – the time left until the **Time limit for the initial connection denial** will be met

Detected threats

Threat log offers detailed information about infiltrations detected by ESET Mail Security modules. The information includes the time of detection, scanner type, object type, object name, infiltration name, location, the performed action and the name of the user logged in at the time the infiltration was detected. To copy or delete one or more lines from the log (or to delete the whole log), use the context menu (right-click on the item).

Events

The Event log contains information about events and errors that have occurred in the program. Often the information found here can help you find a solution for a problem occurring in the program.

On-demand computer scan

The scanner log stores information about manual or planned scan results. Each line corresponds to a single computer control. It lists the following information: scan date and time, total number of scanned, infected, and cleaned files and the current scan status.

In **On-demand scanner logs**, double-click the log entry to display its detailed content in a separate window. Use the context menu (right click) to copy one or more marked entries (in all types of logs).

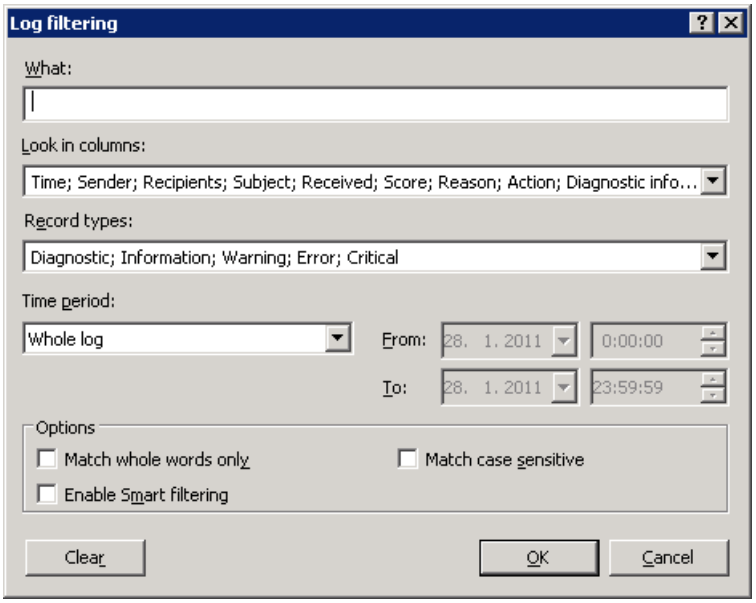
4.5.1 Log filtering

Log filtering is a useful feature that helps you find records in the log files, especially when there are too many records and it is difficult to find the particular information you need.

When using filtering, you can type in a string of **What** to filter, specify what **columns to look in**, select **Record types** and set a **Time period** to narrow down the number of records. By specifying certain filter options, only records that are relevant (according to those filter options) are shown in the **Log files** window for easy and quick access.

To open the **Log filtering** window, press **Filter...** button once in **Tools** > **Log files**, or use shortcut keys Ctrl + Shift + F.

NOTE: To search for a particular record, you can use the Find in log 97 functionality instead, or in conjunction with Log filtering.



By specifying certain filter options, only records that are relevant (according to those filter options) are shown in the Log files window. This will filer out / narrow down the records, thus making it easier for you to find what you are looking for. The more specific filter options you use, the narrower the result will be.

What: - Type in a string (word, or part of a word.) Only records that contain this string will be shown. The rest of the records will not be visible for better readability.

Look in columns: - Select what columns will be taken into account when filtering. You can check one or more columns to be used for filtering. By default, all columns are checked:

- **Time**
- **Module**
- **Event**
- **User**

Record types: - Lets you choose what type of records to show. You can choose one particular record type, multiple types at the same time, or have all of the record types shown (by default):

- **Diagnostic**
- **Information**
- **Warning**
- **Error**
- **Critical**

Time period: - Use this option to have records filtered by time period. You can choose one of the following:

- **Whole log** (default) - does not filter by time period as it shows whole log
- **Last day**
- **Last week**
- **Last month**
- **Interval** - by selecting interval, you can specify exact time period (date and time) to have shown only those record that happened within specified time period.

Apart from the filtering settings above, you also have several **Options**:

Match whole words only - Shows only records that match the string as a whole word in the **What** text box.

Match case sensitive - Shows only records that match the string with exact capitalization in the **What** text box.

Enable Smart filtering - Use this option to let ESET Mail Security perform filtering using its own methods.

Once you are finished with configuring filtering options, press the **OK** button to apply the filter. The **Log files** window will show only corresponding records according to the filter options.

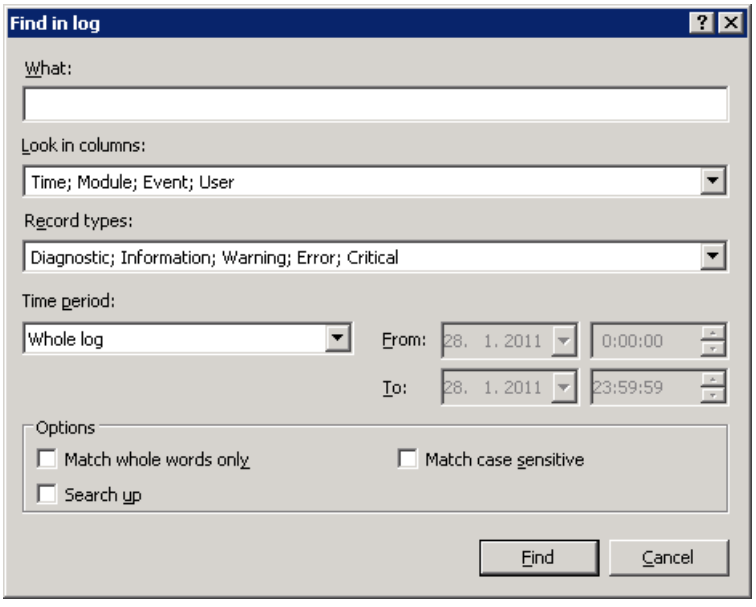
4.5.2 Find in log

In addition to Log filtering 96, you can use search functionality within Log files, however you can also use it independently from log filtering. This is useful when you are looking for particular records in the logs. Like Log filtering, this search feature will help you find the information you are looking for, especially when there are too many records.

When using Find in log, you can type in a string of **What** to find, specify what **columns to look in**, select **Record types** and set a **Time period** to search only for records that happened within that time period. By specifying certain search options, only records that are relevant (according to those search options) will be searched in the Log files window.

In order to search in logs, open the **Find in Log** window by pressing Ctrl + f keys.

NOTE: You can use the Find in log feature in conjunction with Log filtering 96. You can first narrow down the number of records using Log filtering and then start searching only within filtered records.



What: - Type in a string (word, or part of a word). Only records that contain this string will be found. The rest of the

records will be omitted.

Look in columns: - Select what columns will be taken into account when searching. You can check one or more columns to be used for searching. By default, all columns are checked:

- **Time**
- **Module**
- **Event**
- **User**

Record types: - Lets you choose what type of records to find. You can choose one particular record type, multiple types at the same time, or have all of the record types to be searched (by default):

- **Diagnostic**
- **Information**
- **Warning**
- **Error**
- **Critical**

Time period: - Use this option to find records only within particular time period. You can choose one of the following:

- **Whole log** (default) - does not search within time period, searches the whole log
- **Last day**
- **Last week**
- **Last month**
- **Interval** - by selecting interval, you can specify exact time period (date and time) to search only those record that happened within specified time period.

Apart from the find settings above, you also have several **Options**:

Match whole words only - Finds only records that match the string as a whole word in the **What** text box.

Match case sensitive - Finds only records that match the string with exact capitalization in the **What** text box.

Search up - Searches from current position upwards.

Once you configured your search options, click the **Find** button to start searching. The search stops when it finds the first corresponding record. Click the **Find** button again to search further. The Log files are searched from top to bottom, starting from current position (record that is highlighted).

4.5.3 Log maintenance

The Logging configuration of ESET Mail Security is accessible from the main program window. Click **Setup** > **Enter entire advanced setup tree...** > **Tools** > **Log files**. You can specify the following options for log files:

- **Delete records automatically**: Log entries older than the specified number of days are automatically deleted
- **Optimize log files automatically**: Enables automatic defragmentation of log files if the specified percentage of unused records has been exceeded
- **Minimum logging verbosity**: Specifies the logging verbosity level. Available options:

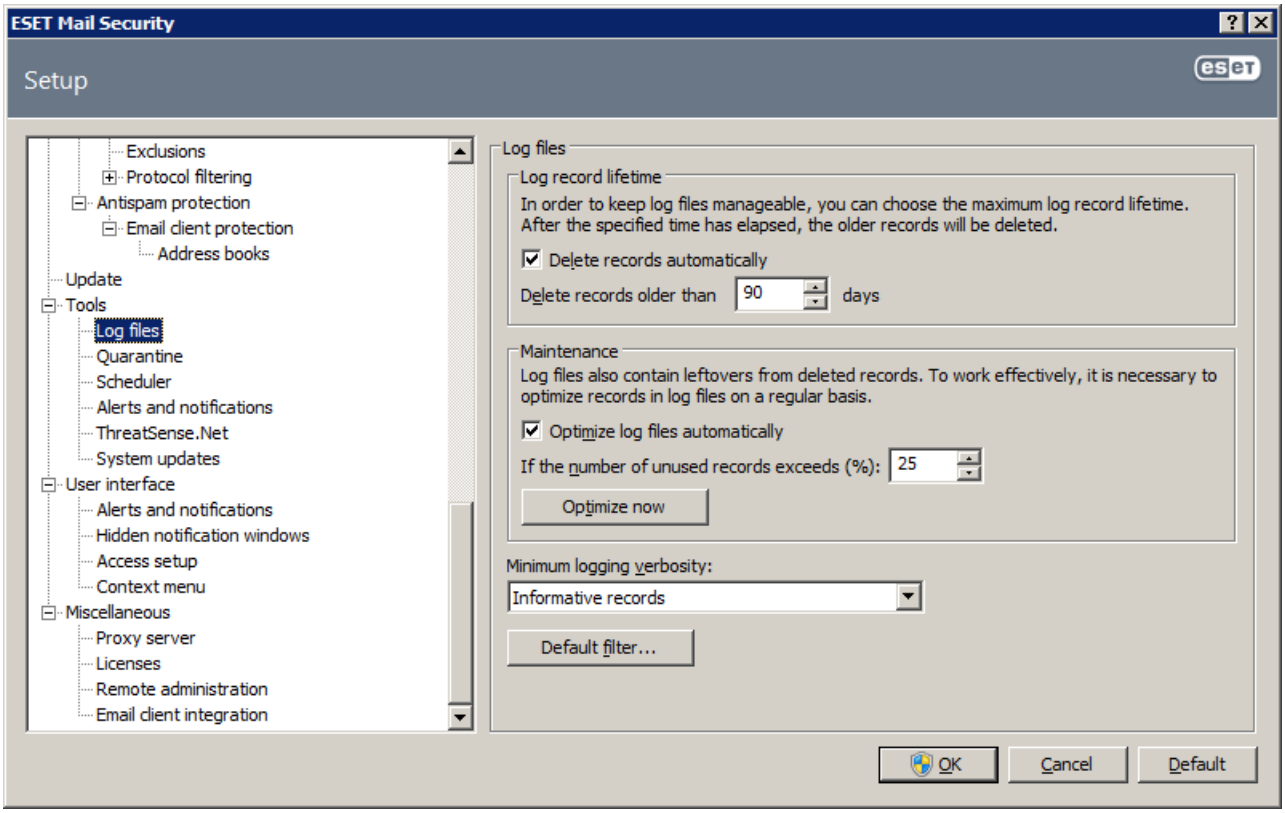
– **Diagnostic records** – Logs information needed for fine-tuning of the program and all records above

– **Informative records** – Records informative messages including successful update messages plus all records above

– **Warnings** – Records critical errors and warning messages

– **Errors** – Only "Error downloading file" messages are recorded, plus critical errors

– **Critical warnings** – Logs only critical errors (error starting Antivirus protection, etc...)



4.6 ESET SysInspector

4.6.1 Introduction to ESET SysInspector

ESET SysInspector is an application that thoroughly inspects your computer and displays gathered data in a comprehensive way. Information like installed drivers and applications, network connections or important registry entries can help you to investigate suspicious system behavior be it due to software or hardware incompatibility or malware infection.

You can access ESET SysInspector two ways: From the integrated version in ESET Security solutions or by downloading the standalone version (SysInspector.exe) for free from ESET's website. Both versions are identical in function and have the same program controls. The only difference is how outputs are managed. The standalone and integrated versions each allow you to export system snapshots to an *.xml* file and save them to disk. However, the integrated version also allows you to store your system snapshots directly in **Tools** > **ESET SysInspector** (except ESET Remote Administrator). For more information see section ESET SysInspector as part of ESET Mail Security 109.

Please allow some time while ESET SysInspector scans your computer. It may take anywhere from 10 seconds up to a few minutes depending on your hardware configuration, operating system and the number of applications installed on your computer.

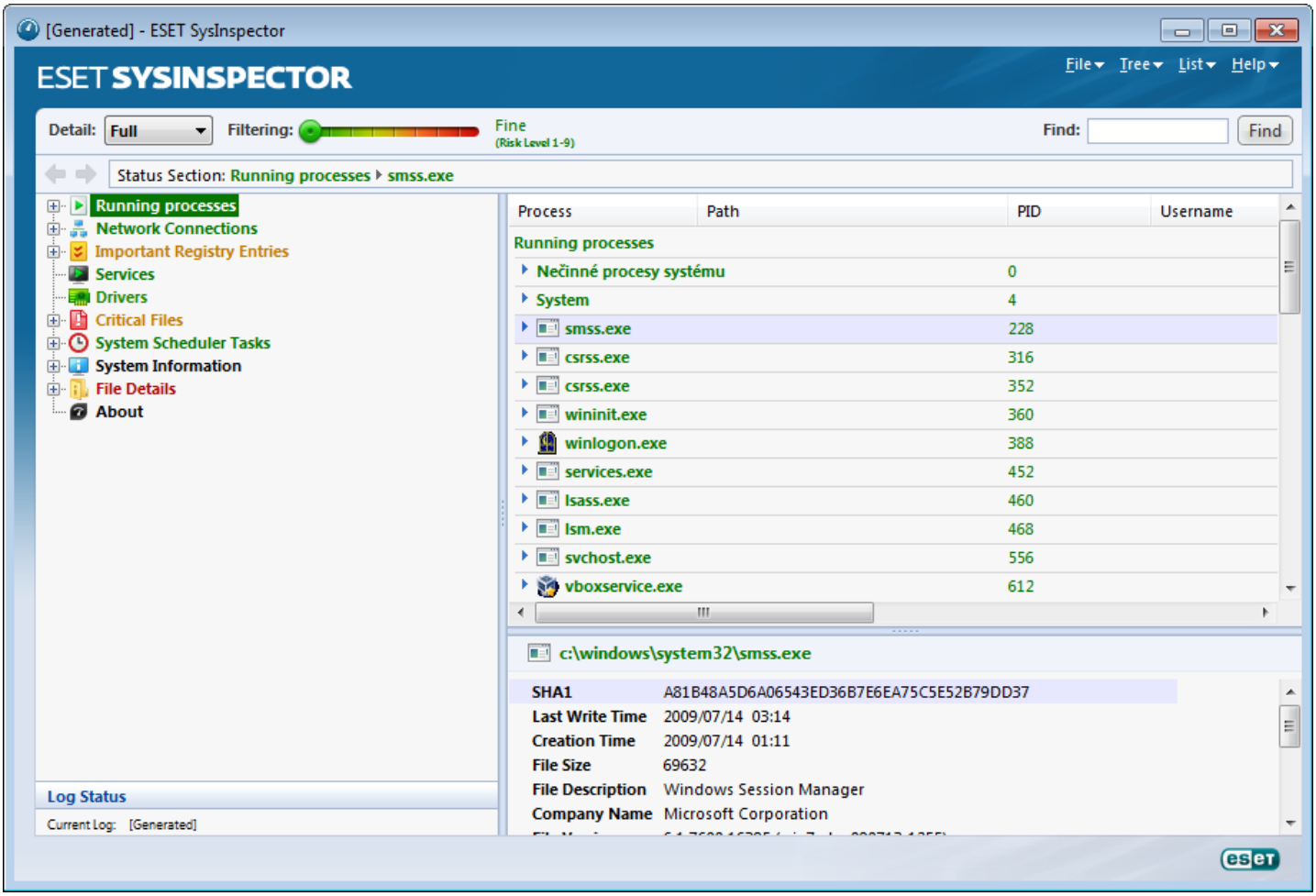
4.6.1.1 Starting ESET SysInspector

To start ESET SysInspector, simply run the *SysInspector.exe* executable you downloaded from ESET's website. If you already have one of the ESET Security solutions installed, you can run ESET SysInspector directly from the Start Menu (**Programs** > **ESET** > **ESET Mail Security**).

Please wait while the application inspects your system, which could take up to several minutes depending on your hardware and data to be gathered.

4.6.2 User Interface and application usage

For clarity the Main window is divided into four major sections – Program Controls located on the top of the Main window, the Navigation window on the left, the Description window on the right in the middle and the Details window on the right at the bottom of the Main window. The Log Status section lists the basic parameters of a log (filter used, filter type, is the log a result of a comparison etc.).



4.6.2.1 Program Controls

This section contains the description of all program controls available in ESET SysInspector.

File

By clicking **File** you can store your current system status for later investigation or open a previously stored log. For publishing purposes we recommend that you generate a log **Suitable for sending**. In this form, the log omits sensitive information (current user name, computer name, domain name, current user privileges, environment variables, etc.).

NOTE: You may open previously stored ESET SysInspector reports by simply dragging and dropping them into the Main window.

Tree

Enables you to expand or close all nodes and export selected sections to Service script.

List

Contains functions for easier navigation within the program and various other functions like finding information online.

Help

Contains information about the application and its functions.

Detail

This setting influences the information displayed in the Main window to make the information easier to work with. In "Basic" mode, you have access to information used to find solutions for common problems in your system. In the "Medium" mode, the program displays less used details. In "Full" mode, ESET SysInspector displays all the information needed to solve very specific problems.

Item filtering

Item filtering is best used to find suspicious files or registry entries in your system. By adjusting the slider, you can filter items by their Risk Level. If the slider is set all the way to the left (Risk Level 1), then all items are displayed. By moving the slider to the right, the program filters out all items less risky than current Risk Level and only display items which are more suspicious than the displayed level. With the slider all the way to the right, the program displays only known harmful items.

All items labeled as risk 6 to 9 can pose security risk. If you are not using a security solution from ESET, we recommend that you scan your system with ESET Online Scanner if ESET SysInspector has found any such item. ESET Online Scanner is a free service.

NOTE: The Risk level of an item can be quickly determined by comparing the color of the item with the color on the Risk Level slider.

Search

Search can be used to quickly find a specific item by its name or part of its name. The results of the search request are displayed in the Description window.

Return

By clicking the back or forward arrow, you may return to previously displayed information in the Description window. You may use the backspace and space keys instead of clicking back and forward.

Status section

Displays the current node in Navigation window.

Important: Items highlighted in red are unknown, which is why the program marks them as potentially dangerous. If an item is in red, it does not automatically mean that you can delete the file. Before deleting, please make sure that files are really dangerous or unnecessary.

4.6.2.2 Navigating in ESET SysInspector

ESET SysInspector divides various types of information into several basic sections called nodes. If available, you may find additional details by expanding each node into its subnodes. To open or collapse a node, double-click the name of the node or alternatively click ⊞ or ⊟ next to the name of the node. As you browse through the tree structure of nodes and subnodes in the Navigation window you may find various details for each node shown in the Description window. If you browse through items in the Description window, additional details for each item may be displayed in the Details window.

The following are the descriptions of the main nodes in the Navigation window and related information in the Description and Details windows.

Running processes

This node contains information about applications and processes running at the time of generating the log. In the Description window you may find additional details for each process such as dynamic libraries used by the process and their location in the system, the name of the application's vendor and the risk level of the file.

The Detail window contains additional information for items selected in the Description window such as the file size or its hash.

NOTE: An operating system comprises of several important kernel components running 24/7 that provide basic and vital functions for other user applications. In certain cases, such processes are displayed in the tool ESET SysInspector with file path beginning with \??\. Those symbols provide pre-launch optimization for those processes; they are safe for the system.

Network connections

The Description window contains a list of processes and applications communicating over the network using the protocol selected in the Navigation window (TCP or UDP) along with the remote address where to which the application is connected to. You can also check the IP addresses of DNS servers.

The Detail window contains additional information for items selected in the Description window such as the file size or its hash.

Important Registry Entries

Contains a list of selected registry entries which are often related to various problems with your system like those specifying startup programs, browser helper objects (BHO), etc.

In the Description window you may find which files are related to specific registry entries. You may see additional details in the Details window.

Services

The Description window Contains a list of files registered as windows Services. You may check the way the service is set to start along with specific details of the file in the Details window.

Drivers

A list of drivers installed in the system.

Critical files

The Description window displays content of critical files related to the Microsoft windows operating system.

System Scheduler Tasks

Contains a list of tasks triggered by Windows Task Scheduler at a specified time/interval.

System information

Contains detailed information about hardware and software along with information about set environmental variables, user rights and system event logs.

File details

A list of important system files and files in the Program Files folder. Additional information specific for the files can be found in the Description and Details windows.

About

Information about version of ESET SysInspector and the list of program modules.

4.6.2.2.1 Keyboard shortcuts

Key shortcuts that can be used when working with the ESET SysInspector include:

File

Ctrl+O	opens existing log
Ctrl+S	saves created logs

Generate

Ctrl+G	generates a standard computer status snapshot
Ctrl+H	generates a computer status snapshot that may also log sensitive information

Item Filtering

1, O	fine, risk level 1-9 items are displayed
2	fine, risk level 2-9 items are displayed
3	fine, risk level 3-9 items are displayed
4, U	unknown, risk level 4-9 items are displayed
5	unknown, risk level 5-9 items are displayed

6	unknown, risk level 6-9 items are displayed
7, B	risky, risk level 7-9 items are displayed
8	risky, risk level 8-9 items are displayed
9	risky, risk level 9 items are displayed
-	decreases risk level
+	increases risk level
Ctrl+9	filtering mode, equal level or higher
Ctrl+O	filtering mode, equal level only

View

Ctrl+5	view by vendor, all vendors
Ctrl+6	view by vendor, only Microsoft
Ctrl+7	view by vendor, all other vendors
Ctrl+3	displays full detail
Ctrl+2	displays medium detail
Ctrl+1	basic display
BackSpace	moves one step back
Space	moves one step forward
Ctrl+W	expands tree
Ctrl+Q	collapses tree

Other controls

Ctrl+T	goes to the original location of item after selecting in search results
Ctrl+P	displays basic information about an item
Ctrl+A	displays full information about an item
Ctrl+C	copies the current item's tree
Ctrl+X	copies items
Ctrl+B	finds information about selected files on the Internet
Ctrl+L	opens the folder where the selected file is located
Ctrl+R	opens the corresponding entry in the registry editor
Ctrl+Z	copies a path to a file (if the item is related to a file)
Ctrl+F	switches to the search field
Ctrl+D	closes search results
Ctrl+E	run service script

Comparing

Ctrl+Alt+O	opens original / comparative log
Ctrl+Alt+R	cancels comparison
Ctrl+Alt+1	displays all items
Ctrl+Alt+2	displays only added items, log will show items present in current log
Ctrl+Alt+3	displays only removed items, log will show items present in previous log
Ctrl+Alt+4	displays only replaced items (files inclusive)
Ctrl+Alt+5	displays only differences between logs
Ctrl+Alt+C	displays comparison
Ctrl+Alt+N	displays current log
Ctrl+Alt+P	opens previous log

Miscellaneous

F1	view help
Alt+F4	close program
Alt+Shift+F4	close program without asking
Ctrl+I	log statistics

4.6.2.3 Compare

The Compare feature allows the user to compare two existing logs. The outcome of this feature is a set of items not common to both logs. It is suitable if you want to keep track of changes in the system, a helpful tool for detecting activity of malicious code.

After it is launched, the application creates a new log which is displayed in a new window. Navigate to **File** > **Save log** to save a log to a file. Log files can be opened and viewed at a later time. To open an existing log, use **File** > **Open log**. In the main program window, ESET SysInspector always displays one log at a time.

The benefit of comparing two logs is that you can view a currently active log and a log saved in a file. To compare logs, use the option **File** > **Compare log** and choose **Select file**. The selected log will be compared to the active one in the main program windows. The comparative log will display only the differences between those two logs.

NOTE: If you compare two log files, select **File** > **Save log** to save it as a ZIP file; both files are saved. If you open this file later, the contained logs are automatically compared.

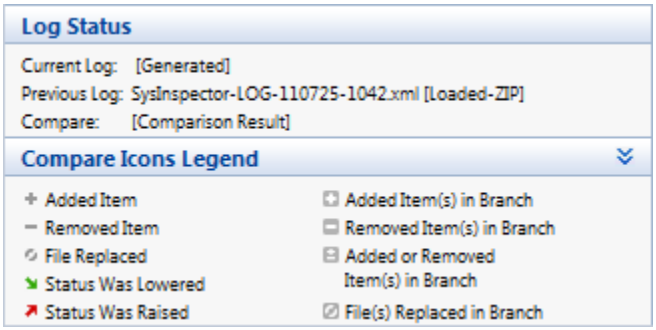
Next to the displayed items, ESET SysInspector shows symbols identifying differences between the compared logs.

Items marked by a − can only be found in the active log and were not present in the opened comparative log. Items marked by a + were present only in the opened log and are missing in the active one.

Description of all symbols that can be displayed next to items:

- + new value, not present in the previous log
- □ tree structure section contains new values
- − removed value, present in the previous log only
- ⊟ tree structure section contains removed values
- ◇ value / file has been changed
- ◪ tree structure section contains modified values / files
- ↘ the risk level has decreased / it was higher in the previous log
- ↗ the risk level has increased / it was lower in the previous log

The explanation section displayed in the left bottom corner describes all symbols and also displays the names of logs which are being compared.



Any comparative log can be saved to a file and opened at a later time.

Example

Generate and save a log, recording original information about the system, to a file named previous.xml. After changes to the system have been made, open ESET SysInspector and allow it to generate a new log. Save it to a file named *current.xml*.

In order to track changes between those two logs, navigate to **File** > **Compare logs**. The program will create a comparative log showing differences between the logs.

The same result can be achieved if you use the following command line option:

SysIsnpector.exe current.xml previous.xml

4.6.3 Command line parameters

ESET SysInspector supports generating reports from the command line using these parameters:

/gen	generate a log directly from the command line without running the GUI
/privacy	generate a log excluding sensitive information
/zip	store the resulting log directly on the disk in a compressed file
/silent	suppress the display of the log generation progress bar
/help, /?	display information about the command line parameters

Examples

To load a specific log directly in the browser, use: *SysInspector.exe "c:\clientlog.xml"*
To generate a log to a current location, use: *SysInspector.exe /gen*
To generate a log to a specific folder, use: *SysInspector.exe /gen="c:\folder\"*
To generate a log to a specific file/location, use: *SysInspector.exe /gen="c:\folder\mynewlog.xml"*
To generate a log excluding sensitive information directly in a compressed file, use: *SysInspector.exe /gen="c:\mynewlog.zip" /privacy /zip*
To compare two logs, use: *SysInspector.exe "current.xml" "original.xml"*

NOTE: If the name of the file/folder contains a gap, then should be taken into inverted commas.

4.6.4 Service Script

Service script is a tool that provides help to customers that use ESET SysInspector by easily removing unwanted objects from the system.

Service script enables the user to export the entire ESET SysInspector log, or its selected parts. After exporting, you can mark unwanted objects for deletion. You can then run the modified log to delete marked objects.

Service Script is suited for advanced users with previous experience in diagnosing system issues. Unqualified modifications may lead to operating system damage.

Example

If you have a suspicion that your computer is infected by a virus which is not detected by your antivirus program, follow the step-by-step instructions below:

- Run ESET SysInspector to generate a new system snapshot.
- Select the first item in the section on the left (in the tree structure), press Ctrl and select the last item to mark all items.
- Right click the selected objects and select the **Export Selected Sections To Service Script** context menu option.
- The selected objects will be exported to a new log.
- This is the most crucial step of the entire procedure: open the new log and change the – attribute to + for all objects you want to remove. Please make sure you do not mark any important operating system files/objects.
- Open ESET SysInspector, click **File** > **Run Service Script** and enter the path to your script.
- Click **OK** to run the script.

4.6.4.1 Generating Service script

To generate a script, right-click any item from the menu tree (in the left pane) in the ESET SysInspector main window. From the context menu, select either the **Export All Sections To Service Script** option or the **Export Selected Sections To Service Script** option.

NOTE: It is not possible to export the service script when two logs are being compared.

4.6.4.2 Structure of the Service script

In the first line of the script's header, you can find information about the Engine version (ev), GUI version (gv) and the Log version (lv). You can use this data to track possible changes in the .xml file that generates the script and prevent any inconsistencies during execution. This part of the script should not be altered.

The remainder of the file is divided into sections in which items can be edited (denote those that will be processed by the script). You mark items for processing by replacing the "-" character in front of an item with a "+" character. Sections in the script are separated from each other by an empty line. Each section has a number and title.

01) Running processes

This section contains a list of all processes running in the system. Each process is identified by its UNC path and, subsequently, its CRC16 hash code in asterisks (*).

Example:

```
01) Running processes:
- \SystemRoot\System32\smss.exe *4725*
- C:\Windows\system32\svchost.exe *FD08*
+ C:\Windows\system32\module32.exe *CF8A*
[...]
```

In this example a process, module32.exe, was selected (marked by a "+" character); the process will end upon execution of the script.

02) Loaded modules

This section lists currently used system modules.

Example:

```
02) Loaded modules:
- c:\windows\system32\svchost.exe
- c:\windows\system32\kernel32.dll
+ c:\windows\system32\khbekhb.dll
- c:\windows\system32\advapi32.dll
[...]
```

In this example the module khbekhb.dll was marked by a "+". When the script runs, it will recognize the processes using that specific module and end them.

03) TCP connections

This section contains information about existing TCP connections.

Example:

```
03) TCP connections:
- Active connection: 127.0.0.1:30606 -> 127.0.0.1:55320, owner: ekrn.exe
- Active connection: 127.0.0.1:50007 -> 127.0.0.1:50006,
- Active connection: 127.0.0.1:55320 -> 127.0.0.1:30606, owner: OUTLOOK.EXE
- Listening on *, port 135 (epmap), owner: svchost.exe
+ Listening on *, port 2401, owner: fservice.exe Listening on *, port 445 (microsoft-ds), owner: System
[...]
```

When the script runs, it will locate the owner of the socket in the marked TCP connections and stop the socket, freeing system resources.

04) UDP endpoints

This section contains information about existing UDP endpoints.

Example:

```
04) UDP endpoints:
- 0.0.0.0, port 123 (ntp)
+ 0.0.0.0, port 3702
- 0.0.0.0, port 4500 (ipsec-msft)
- 0.0.0.0, port 500 (isakmp)
[...]
```

When the script runs, it will isolate the owner of the socket at the marked UDP endpoints and stop the socket.

05) DNS server entries

This section contains information about the current DNS server configuration.

Example:

```
05) DNS server entries:
+ 204.74.105.85
- 172.16.152.2
[...]
```

Marked DNS server entries will be removed when you run the script.

06) Important registry entries

This section contains information about important registry entries.

Example:

```
06) Important registry entries:
* Category: Standard Autostart (3 items)
 HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- HotKeysCmds = C:\Windows\system32\hkcmd.exe
- IgfxTray = C:\Windows\system32\igfxtray.exe
 HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- Google Update = "C:\Users\antoniak\AppData\Local\Google\Update\GoogleUpdate.exe" /c
* Category: Internet Explorer (7 items)
 HKLM\Software\Microsoft\Internet Explorer\Main
+ Default_Page_URL = http://thatcrack.com/
[...]
```

The marked entries will be deleted, reduced to 0-byte values or reset to their default values upon script execution. The action to be applied to a particular entry depends on the entry category and key value in the specific registry.

07) Services

This section lists services registered within the system.

Example:

```
07) Services:
- Name: Andrea ADI Filters Service, exe path: c:\windows\system32\aeadisrv.exe, state: Running, startup:
Automatic
- Name: Application Experience Service, exe path: c:\windows\system32\aelupsvc.dll, state: Running, startup:
Automatic
- Name: Application Layer Gateway Service, exe path: c:\windows\system32\alg.exe, state: Stopped, startup:
Manual
[...]
```

The services marked and their dependant services will be stopped and uninstalled when the script is executed.

08) Drivers

This section lists installed drivers.

Example:

```
08) Drivers:
- Name: Microsoft ACPI Driver, exe path: c:\windows\system32\drivers\acpi.sys, state: Running, startup: Boot
- Name: ADI UAA Function Driver for High Definition Audio Service, exe path: c:\windows\system32
\drivers\adihdaud.sys, state: Running, startup: Manual
[...]
```

When you execute the script, the drivers selected will be stopped. Note that some drivers won't allow themselves to be stopped.

09) Critical files

This section contains information about files that are critical to the operating system.

Example:

```
09) Critical files:
* File: win.ini
- [fonts]
- [extensions]
- [files]
- MAPI=1
[...]
* File: system.ini
- [386Enh]
- woafont=dosapp.fon
- EGA80WOA.FON=EGA80WOA.FON
[...]
* File: hosts
- 127.0.0.1 localhost
- ::1 localhost
[...]
```

The selected items will either be deleted or reset to their original values.

4.6.4.3 Executing Service scripts

Mark all desired items, then save and close the script. Run the edited script directly from the ESET SysInspector main window by selecting the **Run Service Script** option from the File menu. When you open a script, the program will prompt you with the following message: **Are you sure you want to run the service script "%Scriptname%"?** After you confirm your selection, another warning may appear, informing you that the service script you are trying to run has not been signed. Click **Run** to start the script.

A dialog window will confirm that the script was successfully executed.

If the script could only be partially processed, a dialog window with the following message will appear: **The service script was run partially. Do you want to view the error report?** Select **Yes** to view a complex error report listing the operations that were not executed.

If the script was not recognized, a dialog window with the following message will appear: **The selected service script is not signed. Running unsigned and unknown scripts may seriously harm your computer data. Are you sure you want to run the script and carry out the actions?** This may be caused by inconsistencies within the script (damaged heading, corrupted section title, empty line missing between sections etc.). You can either reopen the script file and correct the errors within the script or create a new service script.

4.6.5 FAQ

Does ESET SysInspector require Administrator privileges to run ?

While ESET SysInspector does not require Administrator privileges to run, some of the information it collects can only be accessed from an Administrator account. Running it as a Standard User or a Restricted User will result in it collecting less information about your operating environment.

Does ESET SysInspector create a log file ?

ESET SysInspector can create a log file of your computer's configuration. To save one, select **File** > **Save Log** from the main menu. Logs are saved in XML format. By default, files are saved to the *%USERPROFILE%\My Documents* directory, with a file naming convention of "SysInpsector-%COMPUTERNAME%-YYMMDD-HHMM.XML". You may change the location and name of the log file to something else before saving if you prefer.

How do I view the ESET SysInspector log file ?

To view a log file created by ESET SysInspector, run the program and select **File** > **Open Log** from the main menu. You can also drag and drop log files onto the ESET SysInspector application. If you need to frequently view ESET SysInspector log files, we recommend creating a shortcut to the SYSINSPECTOR.EXE file on your Desktop; you can then drag and drop log files onto it for viewing. For security reasons Windows Vista/7 may not allow drag and drop between windows that have different security permissions.

Is a specification available for the log file format? What about an SDK ?

At the current time, neither a specification for the log file or an SDK are available since the program is still in development. After the program has been released, we may provide these based on customer feedback and demand.

How does ESET SysInspector evaluate the risk posed by a particular object ?

In most cases, ESET SysInspector assigns risk levels to objects (files, processes, registry keys and so forth) using a series of heuristic rules that examine the characteristics of each object and then weight the potential for malicious activity. Based on these heuristics, objects are assigned a risk level from 1 - Fine (green) to 9 - Risky (red). In the left navigation pane, sections are colored based on the highest risk level of an object inside them.

Does a risk level of "6 - Unknown (red)" mean an object is dangerous ?

ESET SysInspector's assessments do not guarantee that an object is malicious – that determination should be made by a security expert. What ESET SysInspector is designed for is to provide a quick assessment for security experts so that they know what objects on a system they may want to further examine for unusual behavior.

Why does ESET SysInspector connect to the Internet when run ?

Like many applications, ESET SysInspector is signed with a digital signature "certificate" to help ensure the software was published by ESET and has not been altered. In order to verify the certificate, the operating system contacts a certificate authority to verify the identity of the software publisher. This is normal behavior for all digitally-signed programs under Microsoft Windows.

What is Anti-Stealth technology ?

Anti-Stealth technology provides effective rootkit detection.

If the system is attacked by malicious code that behaves as a rootkit, the user may be exposed to data loss or theft. Without a special anti-rootkit tool, it is almost impossible to detect rootkits.

Why are there sometimes files marked as "Signed by MS", having a different "Company Name" entry at the same time ?

When trying to identify the digital signature of an executable, ESET SysInspector first checks for a digital signature embedded in the file. If a digital signature is found, the file will be validated using that information. If a digital signature is not found, the ESI starts looking for the corresponding CAT file (Security Catalog - *%systemroot%\system32\catroot*) that contains information about the executable file processed. If the relevant CAT file is found, the digital signature of that CAT file will be applied in the validation process of the executable.

This is why there are sometimes files marked as "Signed by MS", but having a different "CompanyName" entry.

Example:

Windows 2000 includes the HyperTerminal application located in *C:\Program Files\Windows NT*. The main application executable file is not digitally signed, but ESET SysInspector marks it as a file signed by Microsoft. The reason for this is a reference in *C:\WINNT\system32\CatRoot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\sp4.cat* pointing to *C:\Program Files\Windows NT\hypertrm.exe* (the main executable of the HyperTerminal application) and *sp4.cat* is digitally signed by Microsoft.

4.6.6 ESET SysInspector as part of ESET Mail Security

To open the ESET SysInspector section in ESET Mail Security, click **Tools** > **ESET SysInspector**. The management system in the ESET SysInspector window is similar to that of computer scan logs, or scheduled tasks. All operations with system snapshots – create, view, compare, remove and export – are accessible within one or two clicks.

The ESET SysInspector window contains basic information about the created snapshots such as create time, a short comment, name of the user that created the snapshot and snapshot status.

To compare, create, or delete snapshots, use the corresponding buttons located below the list of snapshots in the ESET SysInspector window. Those options are also available from the context menu. To view the selected system snapshot, use the **Show** context menu option. To export the selected snapshot to a file, right-click it and select **Export...**.

Below is a detailed description of the available options:

- **Compare** – Allows you to compare two existing logs. It is suitable if you want to track changes between the current log and an older log. For this option to take effect, you must select two snapshots to be compared.
- **Create...** – Creates a new record. Before that, you must enter a short comment about the record. To find out the snapshot creation progress (of the currently generated snapshot), see the **Status** column. All completed snapshots are marked by the **Created** status.
- **Delete/Delete all** – Removes entries from the list.
- **Export...** – Saves the selected entry in an XML file (also in a zipped version).

4.7 ESET SysRescue

ESET SysRescue is a utility which enables you to create a bootable disk containing one of the ESET Security solutions - it can be ESET NOD32 Antivirus, ESET Smart Security or even some of the server-oriented products. The main advantage of ESET SysRescue is the fact that ESET Security solution runs independent of the host operating system, while it has a direct access to the disk and the entire file system. This makes it possible to remove infiltrations which normally could not be deleted, e.g., when the operating system is running, etc.

4.7.1 Minimum requirements

ESET SysRescue works in the Microsoft Windows Preinstallation Environment (Windows PE) version 2.x, which is based on Windows Vista.

Windows PE is a part of the free packages, Windows Automated Installation Kit (Windows AIK) or Windows Assessment and Deployment Kit (Windows ADK) and therefore Windows AIK or ADK must be installed before creating ESET SysRescue (http://go.eset.eu/AIK) or (http://go.eset.eu/ADK). Which one of these kits should be installed on your system depends on the operating system version you are running. Due to the support of the 32-bit version of Windows PE, it is necessary to use a 32-bit installation package of ESET Security solution when creating ESET SysRescue on 64-bit systems. ESET SysRescue supports Windows AIK 1.1 and higher as well as Windows ADK.

NOTE: Since Windows AIK is over 1 GB in size and Windows ADK is 1.3 GB in size, a high-speed internet connection is required for smooth download.

ESET SysRescue is available in ESET Security solutions version 4.0 and higher.

ESET SysRescue supports following operating systems:

- Windows Server 2003 Service Pack 1 with KB926044
- Windows Server 2003 Service Pack 2
- Windows Server 2008
- Windows Server 2012

Windows AIK supports:

- Windows Server 2003
- Windows Server 2008

Windows ADK supports:

- Windows Server 2012

4.7.2 How to create rescue CD

To launch the ESET SysRescue wizard, click **Start** > **Programs** > **ESET** > **ESET Mail Security** > **ESET SysRescue**.

First, the wizard checks for the presence of Windows AIK or Windows ADK and a suitable device for the boot media creation. If Windows AIK or Windows ADK is not installed on the computer (or it is either corrupt or installed incorrectly), the wizard will offer you the option to install it, or to enter the path to your Windows AIK folder (http://go.eset.eu/AIK) or Windows ADK (http://go.eset.eu/ADK).

NOTE: Since Windows AIK is over 1 GB in size and Windows ADK is 1.3 GB in size, a high-speed internet connection is required for smooth download.

In the next step, select the target media where ESET SysRescue will be located.

4.7.3 Target selection

In addition to CD/DVD/USB, you can choose to save ESET SysRescue in an ISO file. Later on, you can burn the ISO image on CD/DVD, or use it some other way (e.g. in the virtual environment such as VMware or VirtualBox).

If you select USB as the target medium, booting may not work on certain computers. Some BIOS versions may report problems with the BIOS - boot manager communication (e.g. on Windows Vista) and booting exits with the following error message:

```
file : \boot\bcd
status : 0xc000000e
info : an error occurred while attemping to read the boot configuration data
```

If you encounter this message, we recommend selecting CD instead of USB medium.

4.7.4 Settings

Before initiating ESET SysRescue creation, the install wizard displays compilation parameters in the last step of the ESET SysRescue wizard. These can be modified by clicking the **Change...** button. The available options include:

- Folders 111
- ESET Antivirus 111
- Advanced 112
- Internet protocol 112
- Bootable USB device 112 (when the target USB device is selected)
- Burning 112 (when the target CD/DVD drive is selected)

The **Create** button is inactive if no MSI installation package is specified, or if no ESET Security solution is installed on the computer. To select an installation package, click the **Change** button and go to the **ESET Antivirus** tab. Also, if you do not fill in username and password (**Change** > **ESET Antivirus**), the **Create** button is greyed out.

4.7.4.1 Folders

Temporary folder is a working directory for files required during ESET SysRescue compilation.

ISO folder is a folder, where the resulting ISO file is saved after the compilation is completed.

The list on this tab shows all local and mapped network drives together with the available free space. If some of the folders here are located on a drive with insufficient free space, we recommend that you select another drive with more free space available. Otherwise compilation may end prematurely due to insufficient free disk space.

External applications – Allows you to specify additional programs that will be run or installed after booting from a ESET SysRescue medium.

Include external applications – Allows you to add external programs to the ESET SysRescue compilation.

Selected folder – Folder in which programs to be added to the ESET SysRescue disk are located.

4.7.4.2 ESET Antivirus

For creating the ESET SysRescue CD, you can select two sources of ESET files to be used by the compiler.

ESS/EAV folder – Files already contained in the folder to which the ESET Security solution is installed on the computer.

MSI file – Files contained in the MSI installer are used.

Next, you can choose to update the location of (.nup) files. Normally, the default option **ESS/EAV folder/MSI file** should be set. In some cases, a custom **Update folder** can be chosen, e.g., to use an older or newer virus signature database version.

You can use one of the following two sources of username and password:

Installed ESS/EAV – Username and password will be copied from the currently installed ESET Security solution.

From user – Username and password entered in the corresponding text boxes will be used.

NOTE: ESET Security solution on the ESET SysRescue CD is updated either from the Internet or from the ESET

Security solution installed on the computer on which the ESET SysRescue CD is run.

4.7.4.3 Advanced settings

The **Advanced** tab lets you optimize the ESET SysRescue CD according to the amount of memory on your computer. Select **576 MB and more** to write the content of the CD to the operating memory (RAM). If you select **less than 576 MB**, the recovery CD will be permanently accessed when WinPE will be running.

In the **External drivers** section, you can insert drivers for your specific hardware (usually network adapter). Although WinPE is based on Windows Vista SP1, which supports a large range of hardware, occasionally hardware is not recognized. This will required that you add a driver manually. There are two ways of introducing a driver into an ESET SysRescue compilation - manually (the **Add** button) and automatically (the **Aut. Search** button). In the case of manual inclusion, you need to select the path to the corresponding .inf file (applicable *.sys file must also be present in this folder). In the case of automatic introduction, the driver is found automatically in the operating system of the given computer. We recommend using automatic inclusion only if ESET SysRescue is used on a computer that has the same network adapter as the computer on which the ESET SysRescue CD was created. During creation, the ESET SysRescue driver is introduced into the compilation so you do not need to look for it later.

4.7.4.4 Internet protocol

This section allows you to configure basic network information and set up predefined connections after ESET SysRescue.

Select **Automatic private IP address** to obtain the IP address automatically from DHCP (Dynamic Host Configuration Protocol) server.

Alternatively, this network connection can use a manually specified IP address (also known as a static IP address). Select **Custom** to configure the appropriate IP settings. If you select this option, you must specify an **IP address** and, for LAN and high-speed Internet connections, a **Subnet mask**. In **Preferred DNS server** and **Alternate DNS server**, type the primary and secondary DNS server addresses.

4.7.4.5 Bootable USB device

If you have selected a USB device as your target medium, you can select one of the available USB devices on the **Bootable USB device** tab (in case there are more USB devices).

Select the appropriate target **Device** where ESET SysRescue will be installed.

Warning: The selected USB device will be formatted during the creation of ESET SysRescue. All data on the device will be deleted.

If you choose the **Quick format** option, formatting removes all the files from the partition, but does not scan the disk for bad sectors. Use this option if your USB device has been formatted previously and you are sure that it is not damaged.

4.7.4.6 Burn

If you have selected CD/DVD as your target medium, you can specify additional burning parameters on the **Burn** tab.

Delete ISO file – Check this option to delete the temporary ISO file after the ESET SysRescue CD is created.

Deletion enabled – Enables you to select fast erasing and complete erasing.

Burning device – Select the drive to be used for burning.

Warning: This is the default option. If a rewritable CD/DVD is used, all the data on the CD/DVD will be erased.

The Medium section contains information about the medium in your CD/DVD device.

Burning speed – Select the desired speed from the drop-down menu. The capabilities of your burning device and the type of CD/DVD used should be considered when selecting the burning speed.

4.7.5 Working with ESET SysRescue

For the rescue CD/DVD/USB to work effectively, you must start your computer from the ESET SysRescue boot media. Boot priority can be modified in the BIOS. Alternatively, you can use the boot menu during computer startup – usually using one of the F9 - F12 keys depending on the version of your motherboard/BIOS.

After booting up from the boot media, ESET Security solution will start. Since ESET SysRescue is used only in specific situations, some protection modules and program features present in the standard version of ESET Security solution are not needed; their list is narrowed down to **Computer scan**, **Update**, and some sections in **Setup**. The ability to update the virus signature database is the most important feature of ESET SysRescue, we recommend that you update the program prior starting a Computer scan.

4.7.5.1 Using ESET SysRescue

Suppose that computers in the network have been infected by a virus which modifies executable (.exe) files. ESET Security solution is capable of cleaning all infected files except for *explorer.exe*, which cannot be cleaned, even in Safe mode. This is because *explorer.exe*, as one of the essential Windows processes, is launched in Safe mode as well. ESET Security solution would not be able to perform any action with the file and it would remain infected.

In this type of scenario, you could use ESET SysRescue to solve the problem. ESET SysRescue does not require any component of the host operating system, and is therefore capable of processing (cleaning, deleting) any file on the disk.

4.8 User interface options

The user interface configuration options in ESET Mail Security allow you to adjust the working environment to fit your needs. These configuration options are accessible from the **User interface** branch of the ESET Mail Security Advanced Setup tree.

In the **User interface elements** section, the **Advanced mode** option gives users the ability to toggle to Advanced mode. Advanced mode displays more detailed settings and additional controls for ESET Mail Security.

The **Graphical user interface** option should be disabled if the graphical elements slow the performance of your computer or cause other problems. The graphical interface may also need to be turned off for visually impaired users, as it may conflict with special applications that are used for reading text displayed on the screen.

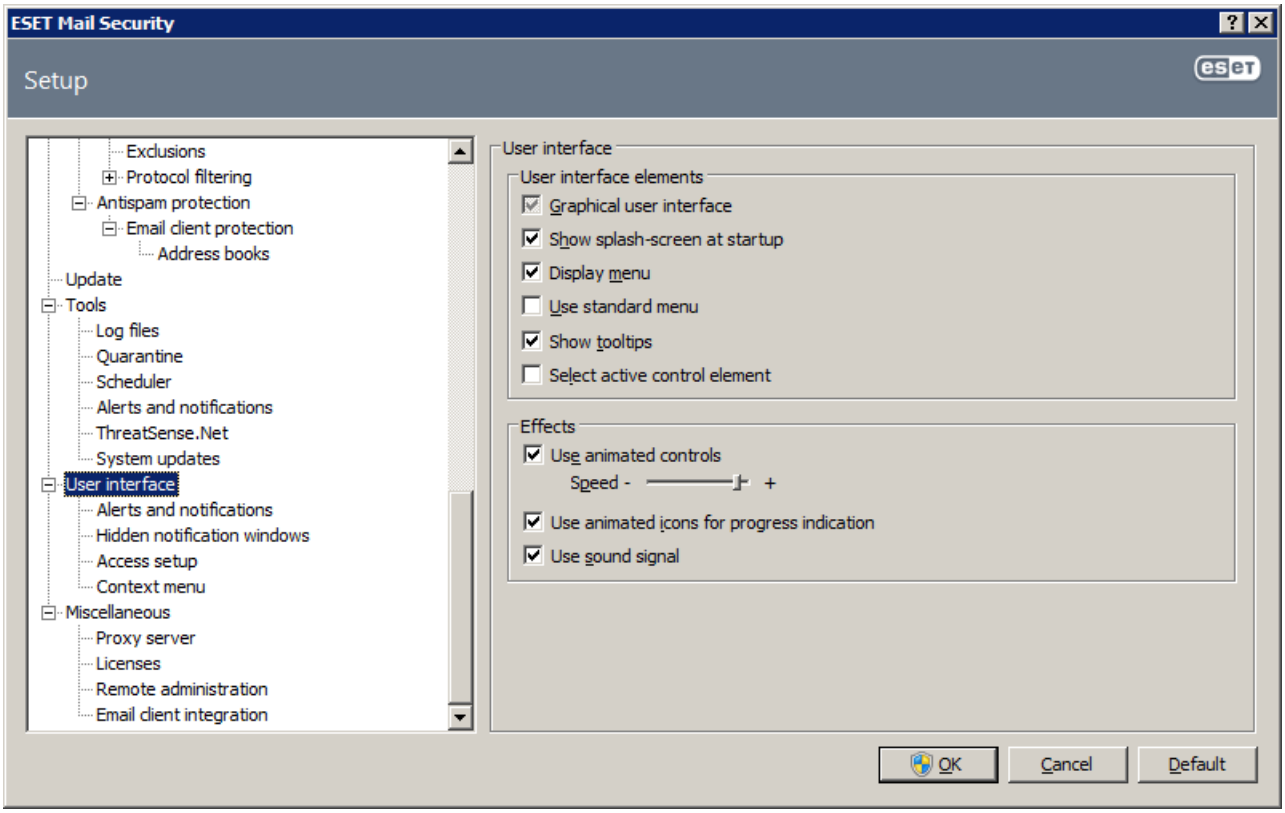
If you wish to disable the ESET Mail Security splash-screen, uncheck the **Show splash-screen at startup** option.

At the top of the ESET Mail Security main program window is a Standard menu which can be activated or disabled based on the **Use standard menu** option.

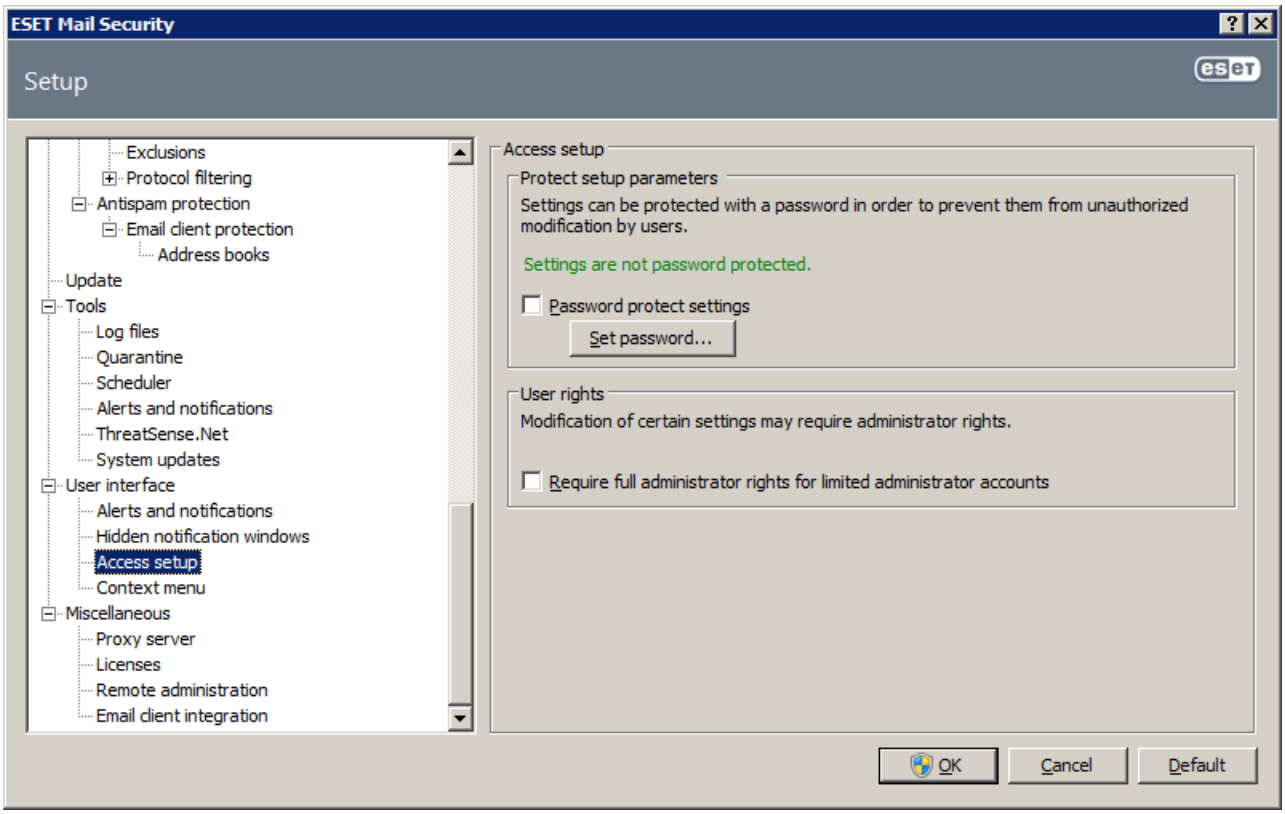
If the **Show tooltips** option is enabled, a short description will be displayed if the cursor is placed over an option. The **Select active control element** option will cause the system to highlight any element which is currently under the active area of the mouse cursor. The highlighted element will be activated after a mouse click.

To decrease or increase the speed of animated effects, select the **Use animated controls** option and move the **Speed** slider bar to the left or right.

To enable the use of animated icons to display the progress of various operations, select the **Use animated icons for progress indication** option. If you want the program to sound a warning if an important event takes place, select the **Use sound signal** option.



The **User interface** features also include the option to password-protect the ESET Mail Security setup parameters. This option is located in the **Settings protection** submenu under **User interface**. In order to provide maximum security for your system, it is essential that the program be correctly configured. Unauthorized modifications could result in the loss of important data. To set a password to protect the setup parameter, click **Set password...**



4.8.1 Alerts and notifications

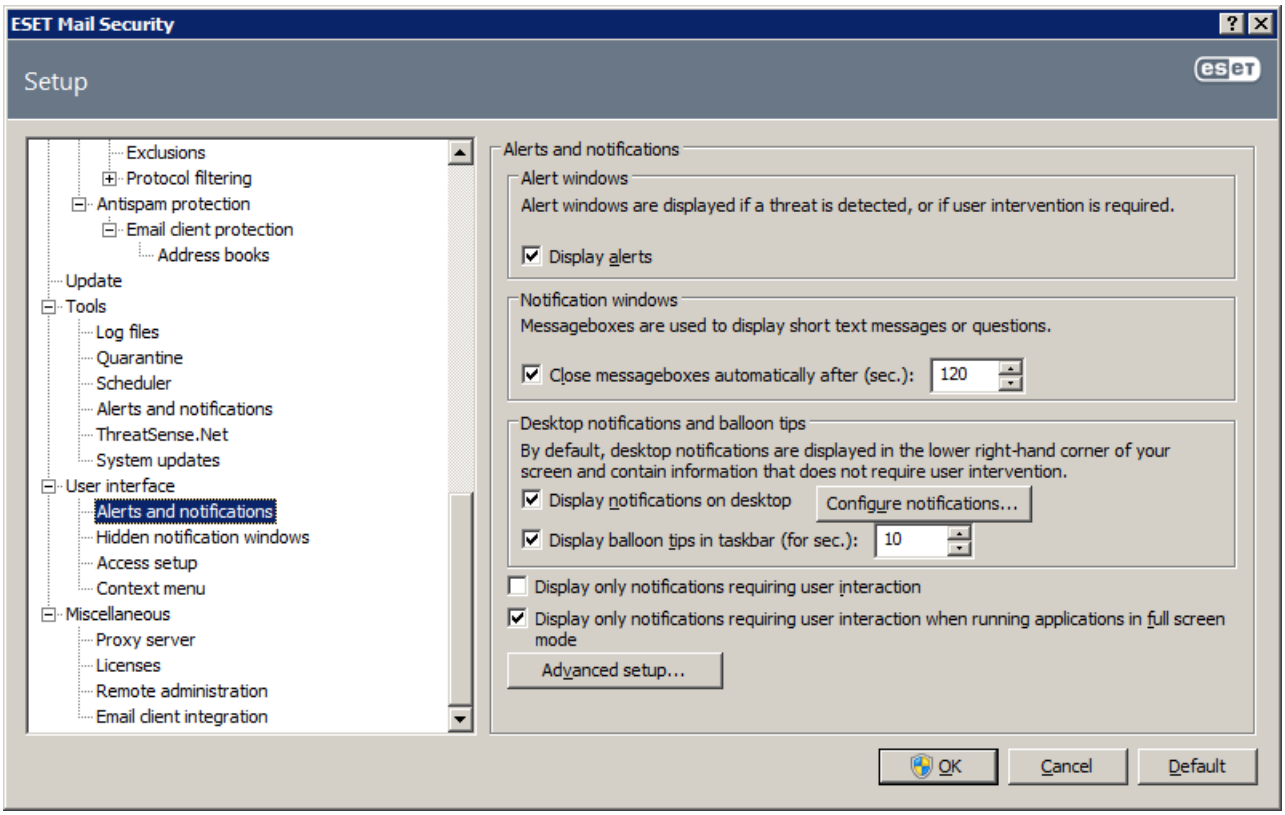
The **Alerts and notifications setup** section under **User interface** allows you to configure how threat alerts and system notifications are handled in ESET Mail Security.

The first item is **Display alerts**. Disabling this option will cancel all alert windows and is only suitable for a limited amount of specific situations. For most users, we recommend that this option be left to its default setting (enabled).

To close pop-up windows automatically after a certain period of time, select the option **Close messageboxes automatically after (sec.)**. If they are not closed manually, alert windows are automatically closed after the specified time period has expired.

Notifications on the Desktop and balloon tips are informative only, and do not require or offer user interaction. They are displayed in the notification area at the bottom right corner of the screen. To activate displaying Desktop notifications, select the **Display notifications on desktop** option. More detailed options – notification display time and window transparency can be modified by clicking the **Configure notifications...** button.

To preview the behavior of notifications, click the **Preview** button. To configure the duration of the balloon tips display time, see the option **Display balloon tips in taskbar (for sec.)**.



Click **Advanced setup...** to enter additional **Alerts and notification** setup options that include the **Display only notifications requiring user's interaction**. This option allows you to turn on/off displaying of alerts and notifications that require no user interaction. Select **Display only notifications requiring user's interaction when running applications in full screen mode** to suppress all noninteractive notifications. From the **Minimum verbosity of events to display** drop-down menu you can select the starting severity level of alerts and notification to be displayed.

The last feature in this section allows you to configure the destination of notifications in a multi-user environment. The **On multi-user systems**, **display notifications on the screen of the user**: field allows you to define who will receive important notifications from ESET Mail Security. Normally this would be a system or network administrator. This option is especially useful for terminal servers, provided that all system notifications are sent to the administrator.

4.8.2 Disable GUI on Terminal Server

This chapter describes how to disable GUI of ESET Mail Security running on Windows Terminal Server for user sessions.

Normally, ESET Mail Security GUI starts up every time a remote user logs onto the server and creates a terminal session. This is usually undesirable on Terminal Servers. If you want to turn off the GUI for terminal sessions follow these steps:

1. Run *regedit.exe*
2. Navigate to *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run*
3. Right-click on Value *egui* and select *Modify...*
4. Add a `/terminal` switch to the end of an existing string

Here is an example of how the Value data of *egui* should be:

```
"C:\Program Files\ESET\ESET Mail Security\egui.exe" /hide /waitservice /terminal
```

If you want to revert this setting and enable automatic startup of the ESET Mail Security GUI, remove the `/terminal` switch. To get to the *egui* registry Value, repeat steps 1. to 3.

4.9 eShell

eShell (short for ESET Shell) is a command line interface for ESET Mail Security. It is an alternative to the graphical user interface (GUI). eShell has all the features and options that the GUI normally gives you. eShell lets you configure and administer the whole program without the use of the GUI.

Apart from all the functions and features that are available in the GUI, it also provides you with the option of using automation by running scripts in order to configure, modify configuration or perform an action. Also, eShell can be useful for those who prefer using the command line over the GUI.

NOTE: A separate manual for eShell is available for you to download here. It lists all the commands with syntax and description.

This section explains how to navigate and use eShell as well as lists all the commands with the description of what particular command is used for and what it does.

There are two modes in which eShell can be run:

- Interactive mode - this is useful when you want to work with eShell (not just execute single command) for tasks such as changing configuration, viewing logs, etc. You can also use interactive mode if you are not familiar with the all the commands yet. Interactive mode will make it easier for you when navigating through eShell. It also shows you available commands you can use within a particular context.
- Single command / Batch mode - you can use this mode if you only need to execute a command without entering the interactive mode of eShell. This can be done from the Windows Command Prompt by typing in `eshell` with appropriate parameters. For example:

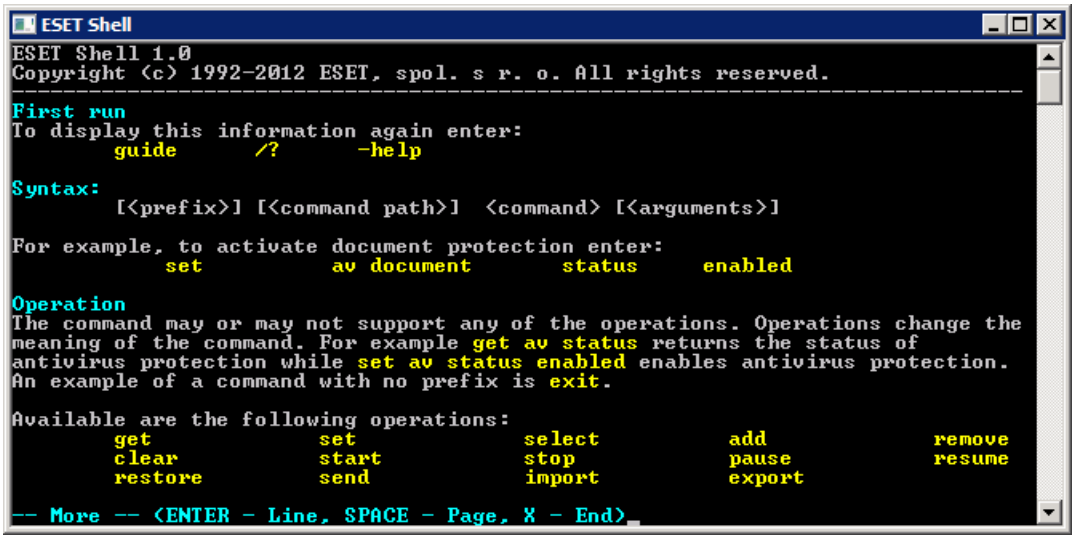
```
eshell set av document status enabled
```

NOTE: In order to run eShell commands from Windows Command Prompt or to run batch files, you need to have this function enabled first (command `set general access batch always` needs to be executed in interactive mode). For further information about the set batch command click here 120.

To enter interactive mode in eShell, you can use one of the following two methods:

- Via Windows Start menu: **Start** > **All Programs** > **ESET** > **ESET File Security** > **ESET shell**
- From Windows Command Prompt by typing in `eshell` and pressing the Enter key

When you run eShell in interactive mode for the first time, a first run screen will display.


ESET Shell
ESET Shell 1.0
Copyright (c) 1992-2012 ESET, spol. s r. o. All rights reserved.
First run
To display this information again enter:
guide /? -help
Syntax:
[<prefix>] [<command path>] <command> [<arguments>]
For example, to activate document protection enter:
set av document status enabled
Operation
The command may or may not support any of the operations. Operations change the meaning of the command. For example get av status returns the status of antivirus protection while set av status enabled enables antivirus protection.
An example of a command with no prefix is exit.
Available are the following operations:
get set select add remove
clear start stop pause resume
restore send import export
-- More -- (ENTER - Line, SPACE - Page, X - End)

It shows you some basic examples how to use eShell with Syntax, Prefix, Command path, Abbreviated forms, Aliases, etc. This is basically a quick guide to eShell.

NOTE: If you want to display the first run screen in future, type in `guide` command.

NOTE: Commands are not case sensitive, you can use upper case (capital) or lower case letters and the command will execute regardless.

4.9.1 Usage

Syntax
Commands must be formatted in the correct syntax to function and can be composed of a prefix, context, arguments, options, etc. This is the general syntax used throughout the eShell:

[<prefix>] [<command path>] <command> [<arguments>]

Example (this activates document protection):
`SET AV DOCUMENT STATUS ENABLED`

`SET` - a prefix
`AV DOCUMENT` - path to a particular command, a context where this command belong
`STATUS` - the command itself
`ENABLED` - an argument for the command

Using `HELP` or `?` with a command will display the syntax for that particular command. For example, `CLEANLEVEL HELP` will show you the syntax for `CLEANLEVEL` command:

SYNTAX:

```
[get] | restore cleanlevel
set cleanlevel none | normal | strict
```

You may notice that `[get]` is in brackets. It designates that the prefix `get` is default for the `cleanlevel` command. This means that when you execute `cleanlevel` without specifying any prefix, it will actually use the default prefix (in this case `get cleanlevel`). Using commands without a prefix saves time when typing. Usually `get` is the default prefix for most commands, but you need to be sure what the default prefix is for particular command and that it is exactly what you want to execute.

NOTE: Commands are not case sensitive, you can use upper case (capital) or lower case letters and the command will execute regardless.

Prefix / Operation
A prefix is an operation. The `GET` prefix will give you information about how a certain feature of ESET Mail Security is configured or show you the status (such as `GET AV STATUS` will show you current protection status). The `SET` prefix will configure functionality or change its status (`SET AV STATUS ENABLED` will activate protection).

These are the prefixes that eShell lets you use. A command may or may not support any of the prefixes:

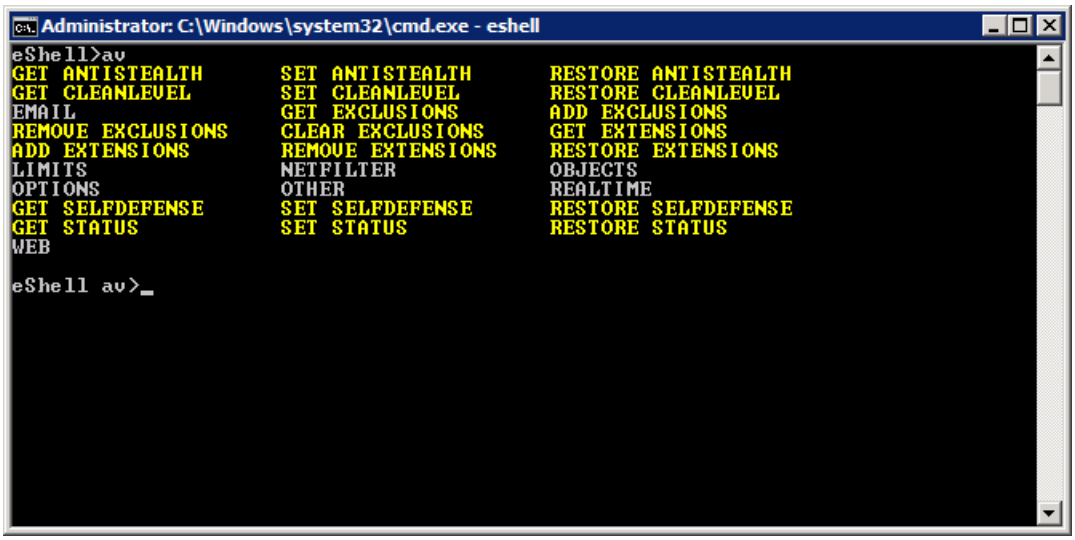
- `GET` - returns current setting/status
- `SET` - sets value/status
- `SELECT` - selects an item
- `ADD` - adds an item
- `REMOVE` - removes an item
- `CLEAR` - removes all items/files
- `START` - starts an action
- `STOP` - stops an action
- `PAUSE` - pauses an action
- `RESUME` - resumes an action
- `RESTORE` - restores default settings/object/file
- `SEND` - sends an object/file
- `IMPORT` - imports from a file
- `EXPORT` - exports to a file

Prefixes such as `GET` and `SET` are used with many commands, but some commands (such as `EXIT`) do not use a prefix.

Command path / Context
Commands are placed in contexts which form a tree structure. The top level of the tree is root. When you run eShell, you are at the root level:

```
eShell>
```

You can either execute a command from here, or enter the context name to navigate within the tree. For example, when you enter `TOOLS` context, it will list all commands and sub-contexts that are available from here.



Yellow items are commands you can execute and grey items are sub-contexts you can enter. A sub-context contain further commands.

If you need to return back to a higher level, use `..` (two dots). For example, say you are here:

```
eShell av options>
```

type `..` and it will get you up one level, to:

```
eShell av>
```

If you want to get back to root from `eShell av options>` (which is two levels lower from root), simply type `.. ..` (two dots and two dots separated by space). By doing so, you will get two levels up, which is root in this case. You can use this no matter how deep within the context tree you are. Use the appropriate number of `..` as you need to get to the desired level.

The path is relative to the current context. If the command is contained in the current context, do not enter a path. For example, to execute `GET AV STATUS` enter:

- `GET AV STATUS` - if you are in the root context (command line shows `eShell>`)
- `GET STATUS` - if you are in the context `AV` (command line shows `eShell av>`)
- `.. GET STATUS` - if you are in the context `AV OPTIONS` (command line shows `eShell av options>`)

Argument
An argument an action which is performed for a particular command. For example, command CLEANLEVEL can be used with following arguments:

- none - Do not clean
- normal - Standard cleaning
- strict - Strict cleaning

Another example are the arguments ENABLED or DISABLED, which are used to enable or disable a certain feature or functionality.

Abbreviated form / Shortened commands
eShell allows you to shorten contexts, commands and arguments (provided the argument is a switch or an alternative option). It is not possible to shorten a prefix or argument that are concrete values such as a number, name or path.

Examples of the short form:

```
set status enabled    =>    set stat en
add av exclusions C:\path\file.ext    =>    add av exc C:\path\file.ext
```

In a case where two commands or contexts start with same letters (such as ABOUT and AV, and you enter A as shortened command), eShell will not be able to decide which command of these two you want to run. An error message will display and list commands starting with "A" which you can choose from:

```
eShell>a
The following command is not unique: a

The following commands are available in this context:
   ABOUT - Shows information about program
   AV - Changes to context av
```

By adding one or more letters (e.g. AB instead of just A) eShell will execute ABOUT command since it is unique now.

NOTE: When you want to be sure that a command executes the way you need, we recommend that you do not abbreviate commands, arguments, etc. and use the full form. This way it will execute exactly as you need and prevent unwanted mistakes. This is especially true for batch files / scripts.

Aliases
An alias is an alternative name which can be used to execute a command (provided that the command has an alias assigned). There are few default aliases:

- (global) help - ?
- (global) close - exit
- (global) quit - exit
- (global) bye - exit
- warnlog - tools log events
- virlog - tools log detections

"(global)" means that the command can be used anywhere regardless of current context. One command can have multiple aliases assigned, for example command EXIT has alias CLOSE, QUIT and BYE. When you want to exit eShell, you can use the EXIT command itself or any of its aliases. Alias VIRLOG is an alias for command DETECTIONS which is located in TOOLS LOG context. This way the detections command is available from ROOT context, making it easier to access (you don't have to enter TOOLS and then LOG context and run it directly from ROOT).

eShell allows you to define your own aliases.

Protected commands
Some commands are protected and can only be executed after entering a password.

Guide
When you run the GUIDE command, it will display a "first run" screen explaining how to use eShell. This command is available from the ROOT context (eShell>).

Help
When the HELP command is used alone, it will list all available commands with prefixes as well as sub-contexts within the current context. It will also give you a short description to each command / sub-context. When you use HELP as an argument with a particular command (e.g. CLEANLEVEL HELP), it will give you details for that command. It

will display SYNTAX, OPERATIONS, ARGUMENTS and ALIASES for the command with a short description for each.

Command history
eShell keeps history of previously executed commands. This applies only to the current eShell interactive session. Once you exit eShell, the command history will be dropped. Use the Up and Down arrow keys on your keyboard to navigate through the history. Once you find the command you were looking for, you can execute it again, or modify it without having to type in the entire command from the beginning.

CLS / Clear screen
The `CLS` command can be used to clear screen. It works the same way as it does with Windows Command Prompt or similar command line interfaces.

EXIT / CLOSE / QUIT / BYE
To close or exit eShell, you can use any of these commands (`EXIT`, `CLOSE`, `QUIT` or `BYE`).

4.9.2 Commands

This section lists few basic eShell commands with description as an example. For the complete list of commands see eShell manual which can be downloaded here.

NOTE: Commands are not case sensitive, you can use upper case (capital) or lower case letters and the command will execute regardless.

Commands contained within **ROOT** context:

ABOUT

Lists information about the program. It shows name of the product installed, version number, installed components (including version number of each component) and basic information about the server and the operating system that ESET Mail Security is running on.

CONTEXT PATH:

```
root
```

BATCH

Starts eShell batch mode. This is very useful when running batch files / scripts and we recommend using it with batch files. Put `START BATCH` as the first command in the batch file or script to enable batch mode. When you enable this function, no interactive input is prompted (e.g. entering a password) and missing arguments are replaced by defaults. This ensures that the batch file will not stop in the middle because eShell is expecting the user to do something. This way the batch file should execute without stopping (unless there is an error or the commands within the batch file are incorrect).

CONTEXT PATH:

```
root
```

SYNTAX:

```
[start] batch
```

OPERATIONS:

`start` - Starts eShell in batch mode

CONTEXT PATH:

```
root
```

EXAMPLES:

`start batch` - Starts eShell batch mode

GUIDE

Displays first run screen.

CONTEXT PATH:

```
root
```

PASSWORD

Normally, to execute password-protected commands, you are prompted to type in a password for security reasons. This applies to commands such as those that disable antivirus protection and those that may affect ESET Mail Security functionality. You will be prompted for password every time you execute such command. You can define this password in order to avoid entering password every time. It will be remembered by eShell and automatically be used when a password-protected command is executed. This means that you do not have to enter the password every time.

NOTE: Defined password works only for the current eShell interactive session. Once you exit eShell, this defined password will be dropped. When you start eShell again, the password needs to be defined again.

This defined password is also very useful when running batch files / scripts. Here is an example of a such batch file:

```
eshell start batch "&" set password plain <yourpassword> "&" set status disabled
```

This concatenated command above starts a batch mode, defines password which will be used and disables protection.

CONTEXT PATH:

```
root
```

SYNTAX:

```
[get] | restore password
```

```
set password [plain <password>]
```

OPERATIONS:

`get` - Show password

`set` - Set or clear password

`restore` - Clear password

ARGUMENTS:

`plain` - Switch to enter password as parameter

`password` - Password

EXAMPLES:

`set password plain <yourpassword>` - Sets a password which will be used for password-protected commands

`restore password` - Clears password

EXAMPLES:

`get password` - Use this to see whether the password is configured or not (this is only shows only stars "*", does not list the password itself), when no stars are visible, it means that there is no password set

`set password plain <yourpassword>` - Use this to set defined password

`restore password` - This command clears defined password

STATUS

Shows information about the current protection status of ESET Mail Security (similar to GUI).

CONTEXT PATH:

```
root
```

SYNTAX:

```
[get] | restore status
```

```
set status disabled | enabled
```

OPERATIONS:

`get` - Show antivirus protection status

`set` - Disable/Enable antivirus protection

`restore` - Restores default settings

ARGUMENTS:

`disabled` - Disable antivirus protection

`enabled` - Enable antivirus protection

EXAMPLES:

`get status` - Shows current protection status

`set status disabled` - Disables protection

`restore status` - Restores protection to default setting (Enabled)

VIRLOG

This is an alias of the `DETECTIONS` command. It is useful when you need to view information about detected infiltrations.

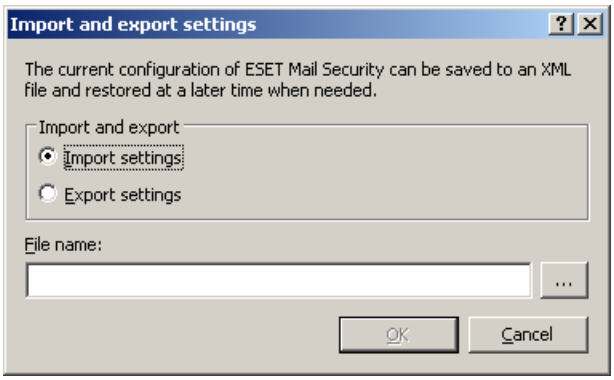
WARNLOG

This is an alias of the `EVENTS` command. It is useful when you need to view information about various events.

4.10 Import and export settings

Importing and exporting configurations of ESET Mail Security is available under **Setup** by clicking on **Import and export settings**.

Both import and export use the .xml file type. Import and export are useful if you need to backup the current configuration of ESET Mail Security to be able to use it later. The export settings option is also convenient for users who wish to use their preferred configuration of ESET Mail Security on multiple systems - they can easily import an .xml file to transfer the desired settings.


Import and export settings
The current configuration of ESET Mail Security can be saved to an XML file and restored at a later time when needed.
Import and export
Import settings
Export settings
File name:
...
OK
Cancel

4.11 ThreatSense.Net

The ThreatSense.Net Early Warning System keeps ESET immediately and continuously informed about new infiltrations. The bidirectional ThreatSense.Net Early Warning System has a single purpose – to improve the protection that we can offer you. The best way to ensure that we see new threats as soon as they appear is to "link" to as many to as many of our customers as possible and use them as our Threat Scouts. There are two options:

1. You can decide not to enable the ThreatSense.Net Early Warning System. You will not lose any functionality in the software, and you will still receive the best protection that we offer.

2. You can configure the ThreatSense.Net Early Warning System to submit anonymous information about new threats and where the new threatening code is contained. This file can be sent to ESET for detailed analysis. Studying these threats will help ESET update its threat detection capabilities.

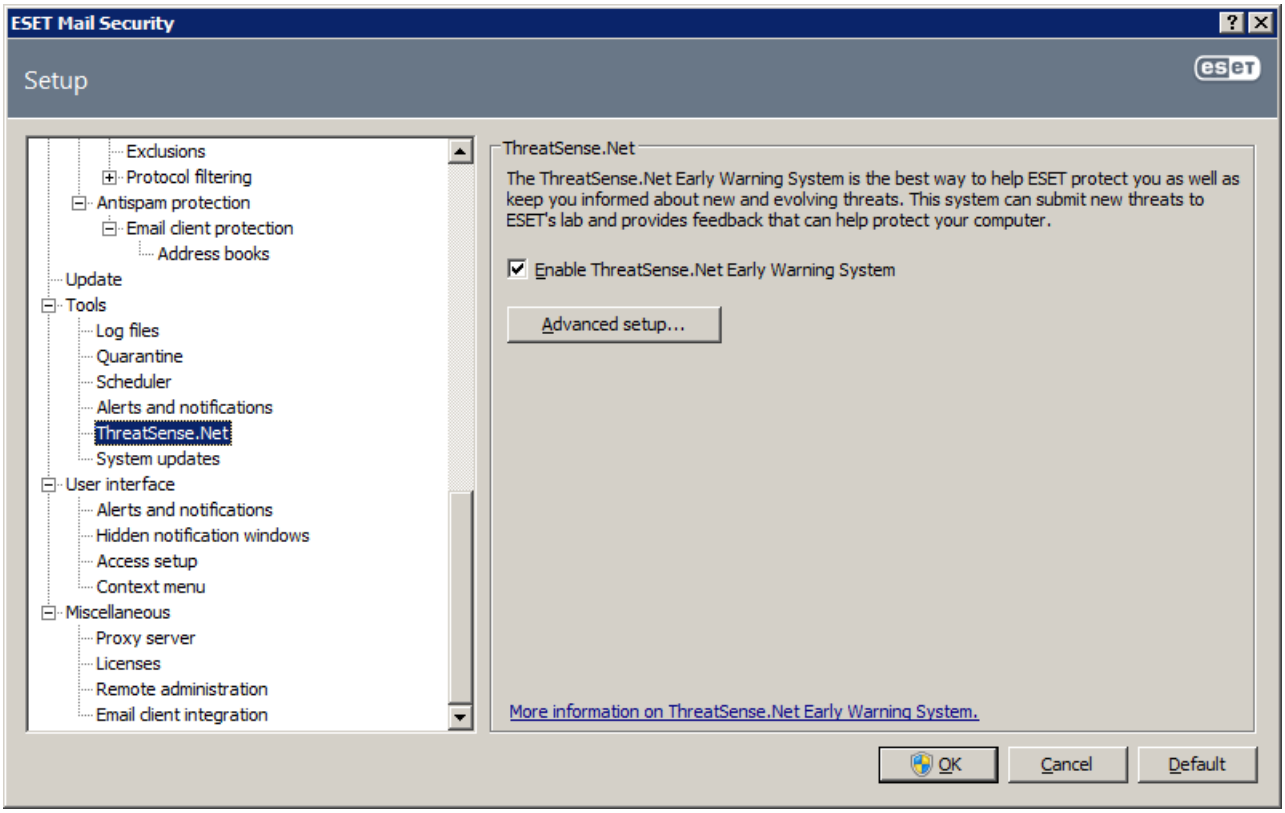
The ThreatSense.Net Early Warning System will collect information about your computer related to

newly-detected threats. This information may include a sample or copy of the file in which the threat appeared, the path to that file, the filename, the date and time, the process by which the threat appeared on your computer and information about your computer's operating system.

While there is a chance that this may occasionally disclose some information about you or your computer (usernames in a directory path, etc.) to ESET's Threat Lab, this information will not be used for ANY purpose other than to help us respond immediately to new threats.

By default, ESET Mail Security is configured to ask before submitting suspicious files for detailed analysis to ESET's Threat Lab. Files with certain extensions such as .doc or .xls are always excluded. You can also add other extensions if there are particular files that you or your organization wants to avoid sending.

The ThreatSense.Net setup is accessible from the Advanced Setup tree, under **Tools** > **ThreatSense.Net**. Select the **Enable ThreatSense Early Warning System** option to activate and then click the **Advanced setup...** button.

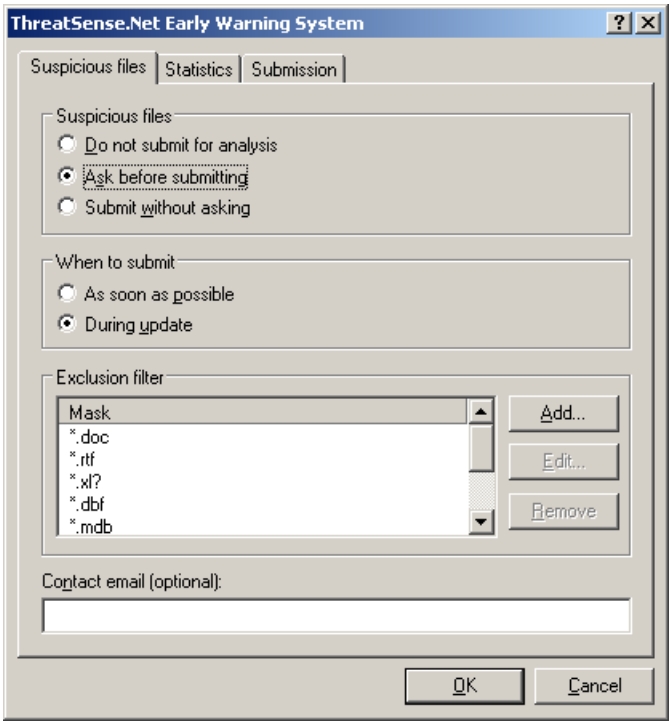


4.11.1 Suspicious files

The **Suspicious files** tab allows you to configure the manner in which threats are submitted to ESET's Threat Lab for analysis.

If you find a suspicious file, you can submit it for analysis to our ThreatLabs. If it is a malicious application, its detection will be added to the next virus signature update.

File submission can be set to occur automatically, or select the **Ask before submitting** option if you wish to know which files have been sent for analysis and confirm the submission.



If you do not want any files to be submitted, select the **Do not submit for analysis** option. Selecting not to submit files for analysis does not affect submission of statistical information which is configured in its own setup (see section Statistics 125).

When to submit – By default, the **As soon as possible** option is selected for suspicious files to be sent to ESET's Threat Lab. This is recommended if a permanent Internet connection is available and suspicious files can be delivered without delay. Select the **During** update option for suspicious files to uploaded to ThreatSense.Net during the next update.

Exclusion filter – The Exclusion filter allows you to exclude certain files/folders from submission. For example, it may be useful to exclude files which may carry confidential information, such as documents or spreadsheets. The most common file types are excluded by default (.doc, etc.). You can add to the list of excluded files if desired.

Contact email – Your **Contact email [optional]** can sent with any suspicious files and may be used to contact you if further information is required for analysis. Please note that you will not receive a response from ESET unless more information is needed.

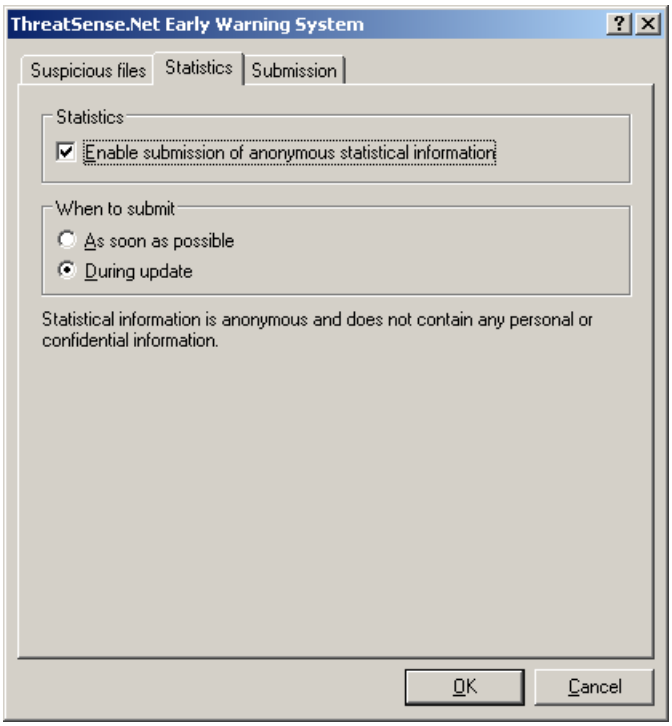
4.11.2 Statistics

The ThreatSense.Net Early Warning System collects anonymous information about your computer related to newly detected threats. This information may include the name of the infiltration, the date and time it was detected, the ESET security product version, your operating system version and the location setting. The statistics are typically delivered to ESET's servers once or twice a day.

Below is an example of a statistical package submitted:

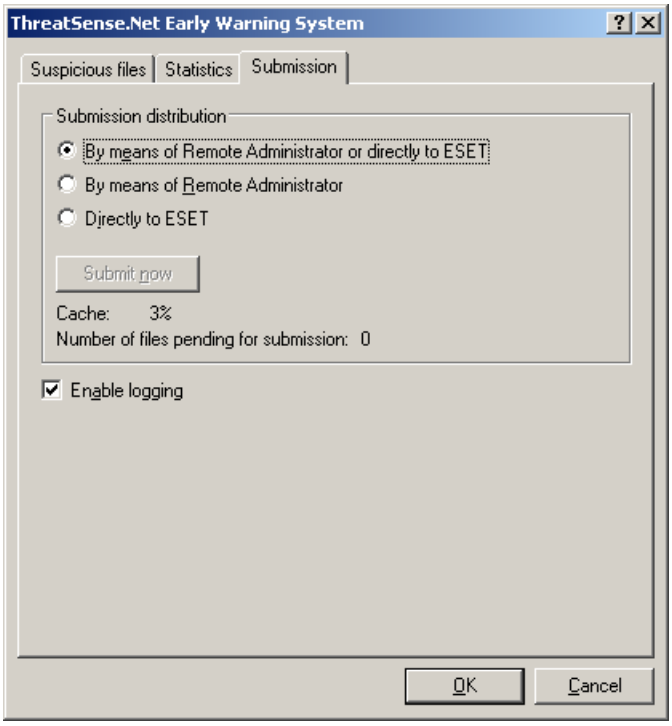
```
# utc_time=2005-04-14 07:21:28
# country="Slovakia"
# language="ENGLISH"
# osver=5.1.2600 NT
# engine=5417
# components=2.50.2
# moduleid=0x4e4f4d41
# filesize=28368
# filename=C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\C14J8NS7\rdgFR1
```

When to submit – You can define when the statistical information will be submitted. If you choose to submit **As soon as possible** statistical information will be sent immediately after it is created. This setting is suitable if a permanent Internet connection is available. If the **During update** option is selected, statistical information will be submitted collectively during the next update.



4.11.3 Submission

You can select how files and statistical information will be submitted to ESET. Select the **By means of Remote Administrator or directly to ESET** option for files and statistics to be submitted by any available means. Select the **By means of Remote Administrator** option to submit files and statistics to the remote administration server, which will ensure their subsequent submission to ESET's Threat Lab. If the option **Directly to ESET** is selected, all suspicious files and statistical information are sent to ESET's virus lab directly from the program.



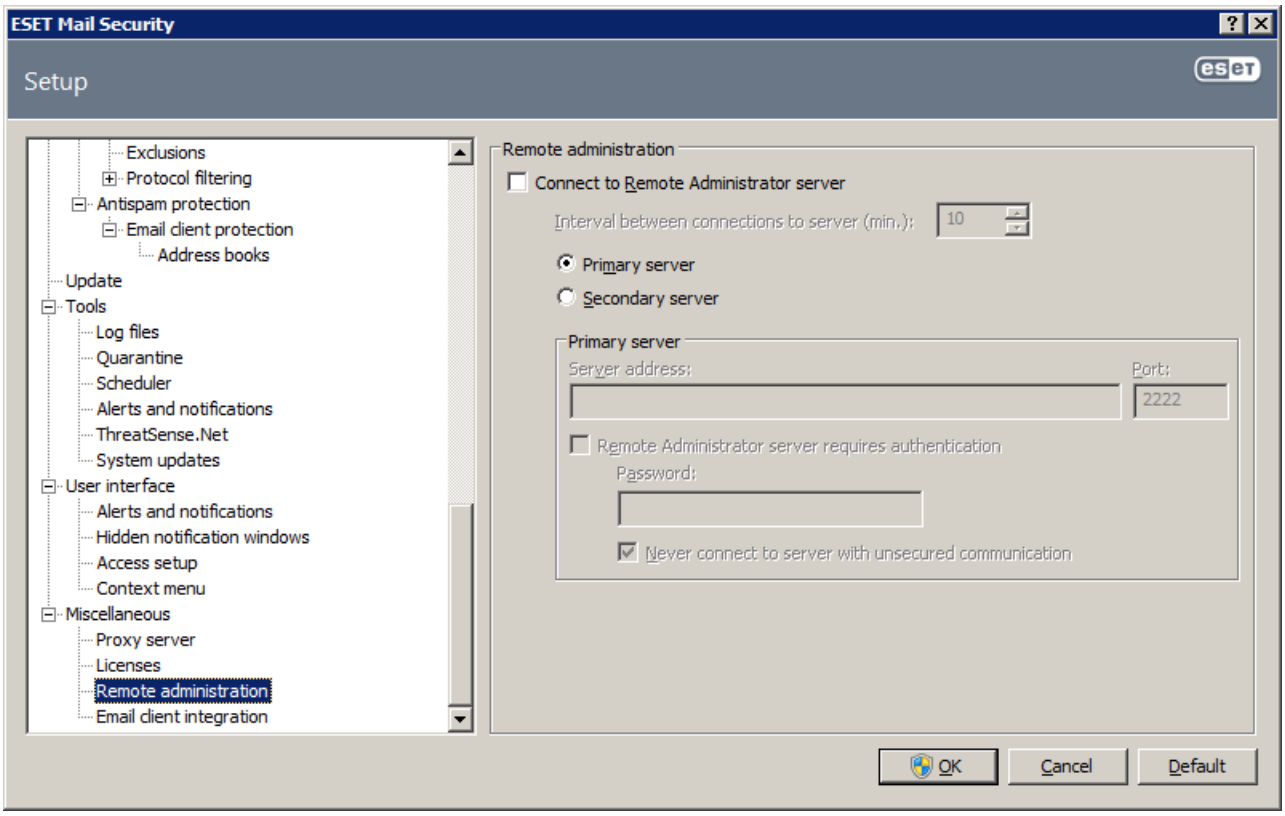
When there are files pending submission, the **Submit now** button will be active. Click this button to immediately submit files and statistical information.

Select the **Enable logging** option to create a log to record file and statistical information submissions.

4.12 Remote administration

ESET Remote Administrator (ERA) is a powerful tool to manage security policy and to obtain an overview of the overall security within a network. It is especially useful when applied to larger networks. ERA not only increases the security level, but also provides ease-of-use in the administration of ESET Mail Security on client workstations.

Remote administration setup options are available from the main ESET Mail Security program window. Click **Setup** > **Enter the entire advanced setup tree...** > **Miscellaneous** > **Remote administration**.



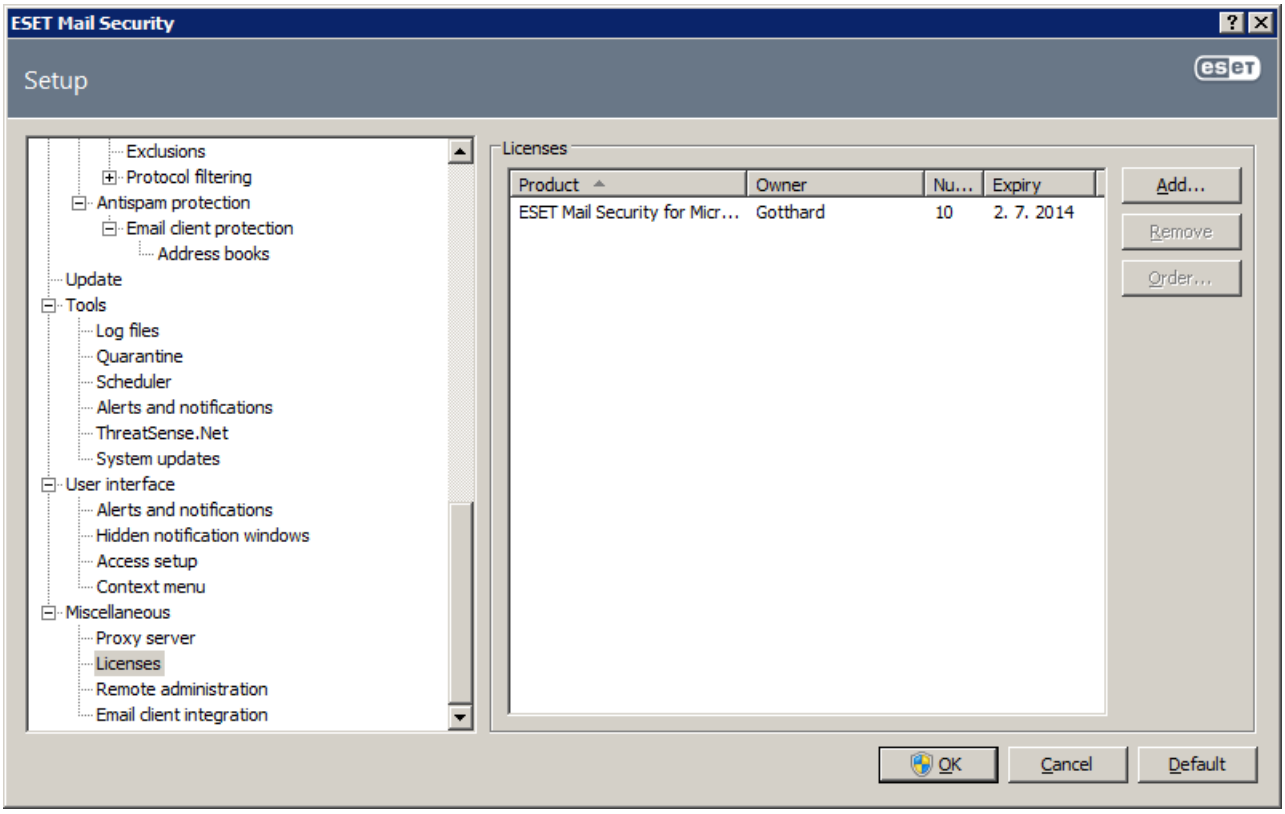
Activate remote administration by selecting the **Connect to Remote Administration server** option. You can then access the other options described below:

- **Interval between connections to server (min.):** This designates the frequency that ESET Mail Security will connect to the ERA Server. If it is set to 0, information will be submitted every 5 seconds.
- **Server address:** Network address of the server where the ERA Server is installed.
- **Port:** This field contains a predefined server port used for connection. We recommend that you leave the default port setting of 2222
- **Remote Administrator server requires authentication:** Allows you to enter a password to connect to the ERA Server, if required.

Click **OK** to confirm changes and apply the settings. ESET Mail Security will use these settings to connect to the ERA Server.

4.13 Licenses

The **Licenses** branch allows you to manage the license keys for ESET Mail Security and other ESET products such as ESET Mail Security, etc. After purchase, license keys are delivered along with your username and password. To **Add/ Remove** a license key, click the corresponding button in the license manager window. The license manager is accessible from the Advanced Setup tree under **Miscellaneous** > **Licenses**.



The license key is a text file containing information about the purchased product: the owner, number of licenses, and the expiration date.

The license manager window allows you to upload and view the content of a license key using the **Add...** button – the information contained is displayed in the manager. To delete license files from the list, click **Remove**.

If a license key has expired and you are interested in purchasing a renewal, click the **Order...** button – you will be redirected to our online store.

5. Glossary

5.1 Types of infiltration

An Infiltration is a piece of malicious software trying to enter and/or damage a user's computer.

5.1.1 Viruses

A computer virus is an infiltration that corrupts existing files on your computer. Viruses are named after biological viruses, because they use similar techniques to spread from one computer to another.

Computer viruses mainly attack executable files and documents. To replicate, a virus attaches its "body" to the end of a target file. In short, this is how a computer virus works: after execution of the infected file, the virus activates itself (before the original application) and performs its predefined task. Only after that is the original application allowed to run. A virus cannot infect a computer unless a user, either accidentally or deliberately, runs or opens the malicious program by him/herself.

Computer viruses can range in purpose and severity. Some of them are extremely dangerous because of their ability to purposely delete files from a hard drive. On the other hand, some viruses do not cause any damage – they only serve to annoy the user and demonstrate the technical skills of their authors.

It is important to note that viruses (when compared to trojans or spyware) are increasingly rare because they are not commercially enticing for malicious software authors. Additionally, the term "virus" is often used incorrectly to cover all types of infiltrations. This usage is gradually being overcome and replaced by the new, more accurate term "malware" (malicious software).

If your computer is infected with a virus, it is necessary to restore infected files to their original state – i.e., to clean them by using an antivirus program.

Examples of viruses are: OneHalf, Tenga, and Yankee Doodle.

5.1.2 Worms

A computer worm is a program containing malicious code that attacks host computers and spreads via a network. The basic difference between a virus and a worm is that worms have the ability to replicate and travel by themselves – they are not dependent on host files (or boot sectors). Worms spread through email addresses in your contact list or exploit security vulnerabilities in network applications.

Worms are therefore much more viable than computer viruses. Due to the wide availability of the Internet, they can spread across the globe within hours or even minutes of their release. This ability to replicate independently and rapidly makes them more dangerous than other types of malware.

A worm activated in a system can cause a number of inconveniences: It can delete files, degrade system performance, or even deactivate programs. The nature of a computer worm qualifies it as a "means of transport" for other types of infiltrations.

If your computer is infected with a worm, we recommend you delete the infected files because they likely contain malicious code.

Examples of well-known worms are: Lovsan/Blaster, Stration/Warezov, Bagle, and Netsky.

5.1.3 Trojan horses

Historically, computer trojan horses have been defined as a class of infiltrations which attempt to present themselves as useful programs, thus tricking users into letting them run. But it is important to note that this was true for trojan horses in the past– oday, there is no longer a need for them to disguise themselves. Their sole purpose is to infiltrate as easily as possible and accomplish their malicious goals. "Trojan horse" has become a very general term describing any infiltration not falling under any specific class of infiltration.

Since this is a very broad category, it is often divided into many subcategories:

- **Downloader** – A malicious program with the ability to download other infiltrations from the Internet
- **Dropper** – A type of trojan horse designed to drop other types of malware onto compromised computers

- **Backdoor** – An application which communicates with remote attackers, allowing them to gain access to a system and to take control of it
- **Keylogger** – (keystroke logger) – A program which records each keystroke that a user types and sends the information to remote attackers
- **Dialer** – Dialers are programs designed to connect to premium-rate numbers. It is almost impossible for a user to notice that a new connection was created. Dialers can only cause damage to users with dial-up modems, which are no longer regularly used

Trojan horses usually take the form of executable files with the extension .exe. If a file on your computer is detected as a trojan horse, it is advisable to delete it, since it most likely contains malicious code.

Examples of well-known trojans are: NetBus, Trojandownloader. Small.ZL, Slapper

5.1.4 Rootkits

Rootkits are malicious programs that grant Internet attackers unlimited access to a system, while concealing their presence. Rootkits, after accessing a system (usually exploiting a system vulnerability), use functions in the operating system to avoid detection by antivirus software: they conceal processes, files and Windows registry data, etc. For this reason, it is almost impossible to detect them using ordinary testing techniques.

There are two levels of detection to prevent rootkits:

1) When they try to access a system. They are still not present, and are therefore inactive. Most antivirus systems are able to eliminate rootkits at this level (assuming that they actually detect such files as being infected).

2) When they are hidden from the usual testing. ESET Mail Security users have the advantage of Anti-Stealth technology, which is also able to detect and eliminate active rootkits.

5.1.5 Adware

Adware is a short for advertising-supported software. Programs displaying advertising material fall under this category. Adware applications often automatically open a new pop-up window containing advertisements in an Internet browser, or change the browser's home page. Adware is frequently bundled with freeware programs, allowing their creators to cover development costs of their (usually useful) applications.

Adware itself is not dangerous – users will only be bothered with advertisements. Its danger lies in the fact that adware may also perform tracking functions (as spyware does).

If you decide to use a freeware product, please pay particular attention to the installation program. The installer will most likely notify you of the installation of an extra adware program. Often you will be allowed to cancel it and install the program without adware.

Some programs will not install without adware, or their functionality will be limited. This means that adware may often access the system in a "legal" way, because users have agreed to it. In this case, it is better to be safe than sorry.If there is a file detected as adware on your computer, it is advisable to delete it, since there is a high probability that it contains malicious code.

5.1.6 Spyware

This category covers all applications which send private information without user consent/awareness. Spyware uses tracking functions to send various statistical data such as a list of visited websites, email addresses from the user's contact list, or a list of recorded keystrokes.

The authors of spyware claim that these techniques aim to find out more about users' needs and interests and allow better-targeted advertisement. The problem is that there is no clear distinction between useful and malicious applications and no one can be sure that the retrieved information will not be misused. The data obtained by spyware applications may contain security codes, PINs, bank account numbers, etc. Spyware is often bundled with free versions of a program by its author in order to generate revenue or to offer an incentive for purchasing the software. Often, users are informed of the presence of spyware during a program's installation to give them an incentive to upgrade to a paid version without it.

Examples of well-known freeware products which come bundled with spyware are client applications of P2P (peer-to-peer) networks. Spyfalcon or Spy Sheriff (and many more) belong to a specific spyware subcategory – they appear to be antispyware programs, but in fact they are spyware programs themselves.

If a file is detected as spyware on your computer, it is advisable to delete it, since there is a high probability that it contains malicious code.

5.1.7 Potentially unsafe applications

There are many legitimate programs whose function is to simplify the administration of networked computers. However, in the wrong hands, they may be misused for malicious purposes. ESET Mail Security provides the option to detect such threats.

"Potentially unsafe applications" is the classification used for commercial, legitimate software. This classification includes programs such as remote access tools, password-cracking applications, and keyloggers 129 (a program that records each keystroke a user types).

If you find that there is a potentially unsafe application present and running on your computer (and you did not install it), please consult your network administrator or remove the application.

5.1.8 Potentially unwanted applications

Potentially unwanted applications are not necessarily intended to be malicious, but may affect the performance of your computer in a negative way. Such applications usually require consent for installation. If they are present on your computer, your system behaves differently (compared to the state before their installation). The most significant changes are:

- New windows you haven't seen previously are opened
- Activation and running of hidden processes
- Increased usage of system resources
- Changes in search results
- Application communicates with remote servers

5.2 Email

Email, or electronic mail, is a modern form of communication with many advantages. It is flexible, fast and direct, and played a crucial role in the proliferation of the Internet in the early 1990's.

Unfortunately, with a high level of anonymity, email and the Internet leave room for illegal activities such as spamming. Spam includes unsolicited advertisements, hoaxes and proliferation of malicious software – malware. The inconvenience and danger to you is increased by the fact that the cost of sending spam is minimal, and authors of spam have many tools to acquire new email addresses. In addition, the volume and variety of spam makes it very difficult to regulate. The longer you use your email address, the more likely it will end up in a spam engine database. Some hints for prevention:

- If possible, don't publish your email address on the Internet
- Only give your email address to trusted individuals
- If possible, don't use common aliases – with more complicated aliases, the probability of tracking is lower
- Don't reply to spam that has already arrived in your inbox
- Be careful when filling out Internet forms – be especially cautious of options such as "Yes, I want to receive information".
- Use "specialized" email addresses – e.g., one for business, one for communication with your friends, etc.
- From time to time, change your email address
- Use an Antispam solution

5.2.1 Advertisements

Internet advertising is one of the most rapidly growing forms of advertising. Its main marketing advantages are minimal costs and a high level of directness; what's more, messages are delivered almost immediately. Many companies use email marketing tools to effectively communicate with their current and prospective customers.

This type of advertising is legitimate, since you may be interested in receiving commercial information about some products. But many companies send unsolicited bulk commercial messages. In such cases, email advertising crosses the line and becomes spam.

The amount of unsolicited email has become a problem and it shows no signs of slowing. Authors of unsolicited email often attempt to disguise spam as legitimate messages.

5.2.2 Hoaxes

A hoax is misinformation which is spread across the Internet. Hoaxes are usually sent via email or communication tools like ICQ and Skype. The message itself is often a joke or Urban Legend.

Computer Virus hoaxes try to generate fear, uncertainty and doubt (FUD) in the recipients, bringing them to believe that there is an "undetectable virus" deleting files and retrieving passwords, or performing some other harmful activity on their system.

Some hoaxes work by asking recipients to forward messages to their contacts, perpetuating the hoax. There are mobile phone hoaxes, pleas for help, people offering to send you money from abroad, etc. It is often impossible to determine the intent of the creator.

If you see a message prompting you to forward it to everyone you know, it may very well be a hoax. There are many websites on the Internet that can verify if an email is legitimate. Before forwarding, perform an Internet search on any message you suspect is a hoax.

5.2.3 Phishing

The term phishing defines a criminal activity which uses techniques of social engineering (manipulating users in order to obtain confidential information). Its aim is to gain access to sensitive data such as bank account numbers, PIN codes, etc.

Access is usually achieved by sending email masquerading as a trustworthy person or business (e.g., financial institution, insurance company). The email can look very genuine, and will contain graphics and content which may have originally come from the source it is impersonating. You will be asked to enter, under various pretenses (data verification, financial operations), some of your personal data – bank account numbers or usernames and passwords. All such data, if submitted, can easily be stolen and misused.

Banks, insurance companies, and other legitimate companies will never request usernames and passwords in an unsolicited email.

5.2.4 Recognizing spam scams

Generally, there are a few indicators which can help you identify spam (unsolicited emails) in your mailbox. If a message fulfills at least some of the following criteria, it is most likely a spam message:

- Sender address does not belong to someone on your contact list
- You are offered a large sum of money, but you have to provide a small sum first
- You are asked to enter, under various pretenses (data verification, Financial operations), some of your personal data – bank account numbers, usernames and passwords, etc.
- It is written in a foreign language
- You are asked to buy a product you are not interested in. If you decide to purchase anyway, please verify that the message sender is a reliable vendor (consult the original product manufacturer)
- Some of the words are misspelled in an attempt to trick your spam filter. For example "vaigra" instead of "viagra", etc

5.2.4.1 Rules

In the context of Antispam solutions and email clients, rules are tools for manipulating email functions. They consist of two logical parts:

1) Condition (e.g., an incoming message from a certain address)

2) Action (e.g., deletion of the message, moving it to a specified folder)

The number and combination of rules varies with the Antispam solution. These rules serve as measures against spam (unsolicited email). Typical examples:

- Condition: An incoming email message contains some of the words typically seen in spam messages 2. Action: Delete the message
- Condition: An incoming email message contains an attachment with an .exe extension 2. Action: Delete the attachment and deliver the message to the mailbox
- Condition: An incoming email message arrives from your employer 2. Action: Move the message to the "Work" folder

We recommend that you use a combination of rules in Antispam programs in order to facilitate administration and to more effectively filter spam.

5.2.4.2 Bayesian filter

Bayesian spam filtering is an effective form of email filtering used by almost all Antispam products. It is able to identify unsolicited email with high accuracy and can work on a per-user basis.

The functionality is based on the following principle: The learning process takes place in the first phase. The user manually marks a sufficient number of messages as legitimate messages or as spam (normally 200/200). The filter analyzes both categories and learns, for example, that spam usually contains the words "rolex" or "viagra", and legitimate messages are sent by family members or from addresses in the user's contact list. Provided that a sufficient number of messages are processed, the Bayesian filter is able to assign a specific "spam index" to each message in order to determine whether it is spam or not.

The main advantage of a Baysesian filter is its flexibility. For example, if a user is a biologist, all incoming emails concerning biology or relative fields of study will generally receive a lower probability index. If a message includes words that would normally qualify it as unsolicited, but it is sent by someone from the user's contact list, it will be marked as legitimate, because senders from a contact list decrease overall spam probability.

5.2.4.3 Whitelist

In general, a whitelist is a list of items or persons who are accepted, or have been granted permission. The term "email whitelist" defines a list of contacts from whom the user wishes to receive messages. Such whitelists are based on keywords searched for in email addresses, domain names, or IP addresses.

If a whitelist works in "exclusivity mode", then messages from any other address, domain, or IP address will not be received. If a whitelist is not exclusive, such messages will not be deleted, but filtered in some other way.

A whitelist is based on the opposite principle to that of a blacklist 133. Whitelists are relatively easy to maintain, more so than blacklists. We recommend that you use both the Whitelist and Blacklist to filter spam more effectively.

5.2.4.4 Blacklist

Generally, a blacklist is a list of unaccepted or forbidden items or persons. In the virtual world, it is a technique enabling acceptance of messages from all users not present on such a list.

There are two types of blacklist. Those created by users within their Antispam application, and a professional, regularly updated blacklists which are created by specialized institutions and can be found on the Internet.

It is essential to use blacklists to successfully block spam, but they are difficult to maintain, since new items to be blocked appear every day. We recommended you use both a whitelist 133 and a blacklist to most effectively filter spam.

5.2.4.5 Server-side control

Server-side control is a technique for identifying mass spam based on the number of received messages and the reactions of users. Each message leaves a unique digital "footprint" based on the content of the message. The unique ID number tells nothing about the content of the email. Two identical messages will have identical footprints, while different messages will have different footprints.

If a message is marked as spam, its footprint is sent to the server. If the server receives more identical footprints (corresponding to a certain spam message), the footprint is stored in the spam footprints database. When scanning incoming messages, the program sends the footprints of the messages to the server. The server returns information on which footprints correspond to messages already marked by users as spam.